宽带中国出版工程

工业和信息产业科技与教育专著出版资金资助出版

# 宽带中国与下一代互联网

曹蓟光　赵　锋　马军锋　编著

電子工業出版社
Publishing House of Electronics Industry
北京・BEIJING

## 内 容 简 介

本书介绍了下一代互联网基础知识，全面分析了下一代互联网组网场景、过渡技术，以及典型的组网方案，综合阐述了未来互联网最新技术方向与典型技术方案，以及“宽带中国战略”与下一代互联网的关系。对于电信运营商、互联网企业及相关高等院校和科研单位的技术管理人员与研发人员从事于互联网技术研究、网络建设与运维、业务创新及相关工作具有重要的参考价值。

本书的主要读者对象是电信运营商、互联网企业及高等院校和科研单位的相关技术管理人员与研发人员。



**图书在版编目（CIP）数据**

宽带中国与下一代互联网 / 曹蓟光，赵锋，马军锋编著. —北京：电子工业出版社，2015.7
（宽带中国出版工程）

ISBN 978-7-121-26435-1

Ⅰ. ①宽… Ⅱ. ①曹… ②赵… ③马… Ⅲ. ①互联网络—研究 Ⅳ. ①TP393.4

中国版本图书馆 CIP 数据核字（2015）第 139188 号

策划编辑：宋 梅
责任编辑：张 京
印 刷：
装 订：
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：720×1 000 1/16 印张：13.5 字数：287.7 千字
版 次：2015 年 7 月第 1 版
印 次：2015 年 7 月第 1 次印刷
印 数：3000 册 定价：49.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

宽带中国出版工程

# 总序 1

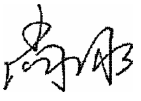
宽带网络是新时期我国经济社会发展的战略性公共基础设施，是推进国家治理能力现代化和公共服务均等化的重要手段，是推动工业强国建设、促进农村经济发展和新型城镇化建设的重要途径。发展宽带网络对于促进信息消费、推动经济发展方式转变、全面建成小康社会具有重要支撑作用。加快宽带网络建设、增强技术创新能力、丰富信息服务应用、繁荣网络文化发展、保障网络安全，利在当前惠及长远。

当前，我国已建成覆盖全国、连接世界、技术先进、全球最大的宽带网络，网民数量、移动智能手机用户规模全球领先，相关产业能力持续提升，已经成为名副其实的网络大国。但同时，我国宽带领域的自主创新能力相对落后，区域和城乡普及差异比较明显，平均带宽与国际先进水平差距较大，网络安全形势日益严峻，总体上看国内宽带网络发展仍存在诸多瓶颈。在全球各国加强宽带战略部署、ICT 产业变革发展日新月异的形势下，要实现工业化、信息化、城镇化、农业现代化四化同步发展、建成网络强国仍然任重道远。

党中央、国务院高度重视宽带网络发展和管理，2013 年国务院先后出台了《“宽带中国”战略及实施方案》和《关于促进信息消费扩大内需的若干意见》。2013 年年底，中央网络安全和信息化领导小组成立，习近平总书记亲自担任组长，提出努力把我国建设成为网络强国，战略部署要与“两个一百年”奋斗目标同步推进，向着网络基础设施基本普及、自主创新能力显著增强、信息经济全面发展、网络安全保障有力的目标不断前进。这是党中央在新时期对我宽带网络发展提出的新目标和新要求，需要我们以改革创新精神，通过政策推动、技术驱动、产业带动、应用拉动促发展保安全；需要我们着眼长远、统筹谋划，积跬步、行千里，不断推动网络大国向网络强国迈进。

工业和信息化部电信研究院是我国在 ICT 领域权威的研究机构，多年来在重大决策支撑、行业发展规划、技术标准引领、产业创新推动和监管支撑服务中发挥了重要作用。“宽带中国出版工程”系列丛书，是该院及业界多位专家学者知识和智慧的结晶，是多专业科研成果的集中展现，更是多年理论与实践经验的综合集成，该系列丛书的出版有助于读者系统学习宽带网络最新技术，准确把握宽带应用和相关产业的最新趋势，从而提升对宽带网络的研究、规划、管理、运营水平。希望我国政产学研用各界齐心协力，共同为宽带中国发展、网络强国建设事业贡献力量！

工业和信息化部



# 总序 2

市场牵引是通信发展的动力，通信业务从话音为主到数据和视频为主，对带宽的需求与日俱增。思科公司 2014 年 6 月发布的报告指出，2013 年全球互联网忙时流量是平均值的 2.66 倍，与 2012 年相比，平均流量和忙时流量分别增长了 25%和 32%，思科公司还预测从 2013 年到 2018 年，全球互联网流量忙时是平均值的 3.22 倍，平均流量和忙时流量分别年增 23%和 28%。在互联网流量中视频已成主流，全球互联网视频流量占总量之比从 2013 年的 57%将增长到 2018 年的 75%。全球移动数据流量增长更快，2013 年一年就增加 81%，到 2018 年还将保持平均年增 61%的速度，届时移动数据流量将占全部 IP 流量的 12%。美国 Telegeography 公司给出的国际互联网干线流量 2009－2013 年平均年增 45%，2013 年相比 2012 年增加了 38%。我国国际互联网干线带宽从 2009 年到 2013 年平均年增 39.6%，2013 年相对 2012 年增 79%，增长的后劲更明显。

通信业务与技术的发展总是市场牵引与技术驱动相辅相成，市场催生了技术，技术支撑了市场。集成电路继续遵循摩尔定律，单位面积的晶体管数年增 40%，强大的计算和处理能力改进了频谱效率与信噪比，提升了通信流量，比较好地适应了互联网流量的增长。光器件的技术进步加上电域的信号处理，使光纤通信干线商用容量水平基本按照十年千倍提升。2009 年起我国移动通信从 2G 经 3G 跨越到 4G，借助先进的多址复用技术和频谱的扩展技术等，峰值速率增加数百倍。

近年通信技术与业务发展一个值得注意的趋势是从消费者的应用向企事业应用扩展，2013 年全球企事业单位互联网流量较 2012 年增 21%，到 2018 年还将达到 2013 年的 2.6 倍，将占全球互联网流量的 14%，而且全球企事业单位互联网流量中 14%将是移动流量。随着物联网发展及信息化与工业化深度融合，企事业单位的互联网应用还将有更大的发展。

互联网的渗透促进了经济的复兴，2013 年发布的《OECD 互联网经济展望 2012》分析了互联网对所有行业经济的影响，得出如果宽带普及率增长 1%，GDP 将增长 0.025%，并且通过模拟得出互联网的贡献占 2010 年美国 GDP 的 4.65%～7.21%，占企业增加值的 3%～13%。波士顿咨询公司 2012 年发表的《连接世界》报告分析 2010－2016 年互联网经济对 GDP 的贡献，中国仅次于英国和韩国为第三位，占 GDP 的比例从 2010 年的 5.5%增加到 2016 年的 6.9%。IDC 公司提出信息技术已从计算机和互联网这两个平台发展到移动宽带、云服务、社交应用和大数据为标志的第三平台，即宽带化平台，并预测到 2020 年信息产业收入的 40%和增长的 98%将由第三平台的技术所驱动。世界银行的研究报告表明，对制造业的海外销售额和服务业的销售额来说，使用宽带的企业与其他企业相比分别高出 6%和 7.5%～10%，中低收入

国家的宽带普及率每增加 10 个百分点，GDP 将会增长 1.38 个百分点。美国认为宽带的发展对上下游产业就业的拉动作用是传统产业的 1.7 倍。GSM 协会和德勤咨询机构 2012 年发表的研究报告指出，3G 移动数据应用增加 100%，人均 GDP 增速提升 1.4 个百分点。

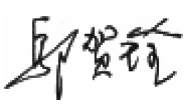
为了抢占信息技术新的制高点并获得宽带化的红利，一些国家纷纷出台国家宽带战略，最近两三年来美国出台了《国家宽带计划》和《大数据研究和发展倡议》等，全球有 146 个国家都制定了加速发展宽带的国家战略或规划，不少国家建立了宽带普遍服务基金。

我国网民数量世界第一，但按网民平均的国际互联网干线带宽、固网平均接入速率和移动互联网下载速率仍低于世界平均水平，这几年有了显著改进，但与互联网高速发展和社会大众的期望相比总是恨铁不成钢。国务院在 2013 年 8 月发布了《“宽带中国”战略及实施方案》，提出到 2015 年要初步建成宽带、融合、安全、泛在的下一代国家信息基础设施，到 2020 年我国下一代信息基础设施基本接近发达国家水平，技术创新和产业竞争力达到国际先进水平。该方案对宽带网络覆盖、网络能力、应用水平、产业链发展和网络信息安全保障五方面提出了具体发展目标、重大任务和保障举措等。可以预期“宽带中国”战略的实施，必将为我国经济和社会的发展奠定坚实的网络基础，并惠及大众。

工业和信息化部电信研究院作为“宽带中国”战略的起草支撑单位之一，为“宽带中国”战略的制定做了深入的调查研究，现在与电子工业出版社联袂推出“宽带中国出版工程”系列丛书。该丛书串起终端、接入、传送、网络和云端各环节，涉及研究、制造、运营与服务各方面，涵盖宽带化技术、业务、应用、安全与管理各领域，解读“宽带中国”战略制定的背景，分析宽带化的解决方案，展望宽带化发展的前景。本套丛书内容全面，系统性强，既反映了宽带网最新的技术及国际标准化进展，又有国内实践经验的总结，兼具前瞻性与实用性。在此，衷心感谢工业和信息化部电信研究院和电子工业出版社及众多的作者所付出的辛勤劳动，希望本套丛书能够有助于业内外人士加深对宽带化的意义和内涵及难度的理解，相信本套丛书能够对行业发展和政府决策起到积极作用，为“宽带中国”战略的实施贡献正能量。

**工业和信息化部通信科学技术委员会主任**

**中国互联网协会理事长**



# 前　言

宽带是 21 世纪人类社会新的战略性基础设施，正深刻改变着人们的生产、生活方式，成为世界各国提振经济、推进发展方式转型、创造就业和提升国家长期竞争力的战略基石。2013 年 8 月国务院印发了《“宽带中国”战略及实施方案》（国发〔2013〕31 号），作为当前和今后一段时期指导我国宽带发展的战略路线图和行动纲领。

实施“宽带中国”战略，就是要加强国家顶层设计和统筹谋划，凝聚全社会力量，全面推进宽带网络普及提速，加快构建下一代国家信息基础设施，大力促进宽带在国民经济和社会各领域的深化应用，推进信息化和工业化深度融合，形成支撑经济社会发展和科技创新的基础平台和重要动力。下一代互联网发展是实施“宽带中国”战略的重要任务，加快下一代互联网创新发展对于提高我国信息技术领域自主创新能力、提升网络基础设施的服务能力和水平、增强我国信息产业核心竞争力、维护网络空间安全均具有重要意义，是实施“宽带中国”战略的重要抓手。

随着 IPv4 地址资源的枯竭，全球加快了 IPv6 商用部署进程，强化了未来网络体系结构的研究与试验，我国政府也适时明确了下一代发展的路线图和时间表，积极推动现有互联网向下一代互联网的演进，大力开展下一代互联网的规模部署，同时，面向未来互联网的发展需求，积极谋划新型网络体系结构的创新与示范。下一代互联网是未来的发展方向，其中涉及众多新技术和新业务，在下一代互联网发展与演进的过程中，更多的新技术还将不断涌现。

本书坚持“面向前沿、服务实践、兼顾基础”的原则，面向互联网发展方向，介绍并比较分析国内外未来互联网的典型技术方案；面向国内下一代互联网的规模部署需求，重点介绍下一代互联网组网技术和过渡方案；介绍下一代互联网、未来互联网的基础技术知识。为电信运营商、互联网企业、高校与科研单位的管理人员与技术人员从事互联网技术研究、网络建设与运维、业务创新相关工作提供必要的参考资料。

本书 3.1 节～3.5 节由赵锋编写，第 4 章由马军锋编写，其余内容由曹蓟光编写。在本书编写过程中，得到了高巍、朱刚、张健、宋菲等同志的帮助和支持，同时也参考了大量国内外科技文献，在此对这些同志和文献作者一并表示感谢。

编著者

2015 年 4 月于北京

# 目　录

# 第 1 章

# 全球宽带发展及下一代互联网演进

## 本章要点

- ✓ 国际宽带发展情况
- ✓ 典型国家宽带发展战略
- ✓ 中国宽带发展现状
- ✓ 中国宽带发展目标
- ✓ 发展下一代互联网是“宽带中国”战略的重要任务

## 本章导读

20 世纪 90 年代以来，以通信和电子为代表的信息产业成为推动全球经济发展的主要驱动力之一。负责信息高速传递的宽带网络，不仅是电信网、互联网和广播电视网等信息通信网络的基石，而且正在逐渐深入到政治、经济、文化、金融、教育和医疗等各个社会领域，使整个社会生活和经济形态发生了重大变化。而宽带的发展，也从根本上离不开国家战略的推动和相关国家政策的指导。目前，欧、美、日、韩等主要互联网发达国家和地区都已经将宽带网络发展纳入国家战略的高度，纷纷出台一系列相关鼓励政策，努力将社会需求和宽带网络供给形成合力并引导宽带产业链有序快速发展，以此来推动各自国家和地区宽带网络的发展，让全社会更快更好地从宽带的发展中受益。我国也十分重视宽带的发展并且取得了很多成绩，但是与发达国家宽带网络发展状况相比，我国宽带网络的差距依然较大，还有很大的发展空间。

# 1.1 国际宽带发展情况

全球已经对宽带对社会、经济产生的巨大作用达成共识，全球多国推出宽带战略。宽带网络速率的不断提高，将有利于各国网络环境的改善，有助于电子商务、电子政务及电子购物等领域的发展，从而间接推动国家经济的发展。目前，多数国家已经进入到宽带战略实施阶段，相应的配套政策不断推出，资金开始到位。运营商加速网络建设与部署，推出更高速率的服务，全球宽带业务市场强劲增长，宽带战略效果开始显现。

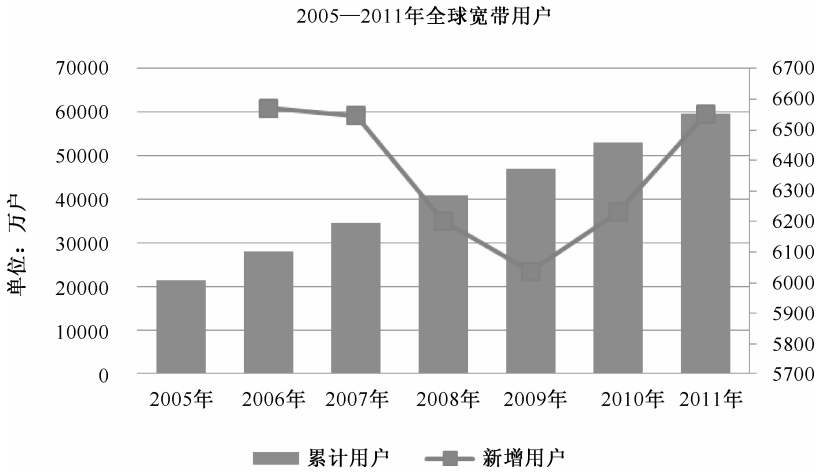
## 1.1.1 宽带市场发展现状

全球宽带用户市场已经达到一定规模。截止到 2011 年年底，全球宽带接入用户累计达到 5.97 亿户，宽带人口普及率达到 10.25%，家庭普及率达到 37.75%。宽带对经济发展的影响越来越大，并成为新一轮技术革命赢得主动权的关键因素。

### 1．全球宽带用户增速快，潜力巨大

全球宽带用户已经从 2010 年开始进入新一轮的用户增长期，用户发展加速，2010 年和 2011 年的新增用户都比上一年有明显增加。未来，全球宽带用户仍将保持增长发展的势头。预计，2012—2016 年年均新增用户将在 8000 万户以上。到 2016 年，

全球宽带接入用户将突破 10 亿户，人口普及率将超过 15%，具体如图 1-1 所示。




数据来源：Point topic。

图 1-1　全球宽带接入累计用户数及新增用户

### 2．发展中国家用户市场份额快速提升，仍与发达国家有很大差距

发展中国家在宽带接入用户市场中的份额已经从 2006 年的 44%提高到 62%。但发展中国家在普及率、价格等方面仍与发达国家有很大差距。

普及率：西欧、北美等发达国家的人口普及率已经超过 30%，而发展中国家和地区的人口普及率仍在 10%左右，具体见图 1-2。

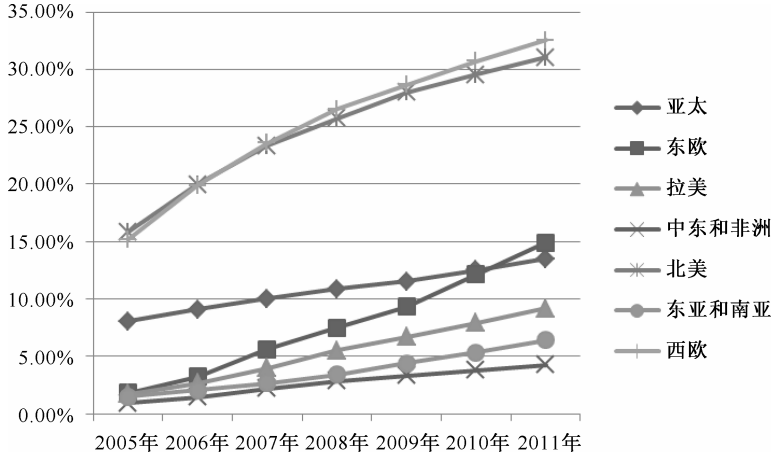



图 1-2　2005—2011 年各地区宽带接入用户普及率

价格：据 ITU 统计，发达国家和地区的宽带入门级资费与人均 GNI 之比基本都在 0.01 以下，而发展中国家和地区的宽带入门级资费与人均 GNI 之比大多在 0.05

以上。

### 3．全球网速大大提升

随着宽带网络的规模建设、FTTx 的不断深入，全球各国宽带接入速率大大提升。Akamai 的监测报告表明，2011 年第四季度全球平均网速同比增长了 19%，达 2.3Mbps，平均峰值网速达 11.7Mbps。在 2011 年第四季度，全球高速宽带（>5 Mbps）的使用率为 27%，同比增长 17%。全球普通宽带（网速大于 2Mbps）的采用率为 66%，同比增长 9.2%。全球窄带上网（网速小于 256Kbps）的采用率继续下降，为 2.5%。

### 4．光进铜退进程加速

高端业务的发展及传输高清视频流的需求走高，接入网中应用 VDSL、PON 替代 ADSL 的进程将不断加快，数据传输速率会越来越快。

全球光接入设备收入近几年增长较快，2011 年为 21 亿美元，市场份额提高幅度较大，从 2008 年的 18%增长到 2011 年的近 30%，成为市场份额第二的技术，并有取代 DSL 位居首位的趋势。

### 5．移动带宽飞速发展

全球各国纷纷通过多种接入手段为用户提供无缝的宽带接入服务，移动宽带近年来飞速发展。根据 ITU 的统计报告，截至 2011 年年底，移动宽带用户将近 12 亿户，过去四年每年增长 45%，用户数已达固定宽带的两倍。

## 1.1.2　全球宽带发展目标

国际社会更加重视宽带的重要作用，加大推进力度。2011 年 10 月，联合国宽带数字发展委员会确定了 2015 年全球宽带发展的 4 个新目标。

① 普遍制定宽带政策。到 2015 年，所有国家均应制定国家宽带计划或战略，或在其普遍接入/服务定义中包括宽带。

② 降低宽带门槛目标。到 2015 年，所有发展中国家应通过合理调控和市场调节，使初级宽带服务的价格达到可接受水平。例如，宽带的支出应当低于人均月收入的 5%。

③ 加大家庭的宽带连接。到 2015 年，发展中国家和地区 40%的家庭应拥有 Internet 接入。

④ 推动居民上网。到 2015 年，全球 Internet 用户普及率应达到 60%，在发展中国家应达到 50%，在最不发达国家（LDC）达到 15%。

2012 年年初，联合国宽带数字发展委员会又呼吁把宽带纳入进经济、环境、社

会三大可持续发展支柱中，用宽带促进全球向可持续、低碳的未来发展。

### 1. 各国宽带战略的制定及目标分析

各国抢抓宽带发展的历史契机，加快制定实施宽带国家战略和行动计划，110 多个国家推出相关计划，各国政府、国际社会高度重视，如“连通美国”、“数字英国”、“数字法国”、“智慧国新加坡”、“i-Japan”等，国际社会以宽带普及、网络提速和应用推进为重点。目前全球发布宽带战略的国家及经济体中以欧洲最多，达到 37 个，在全球占比为 33.6%；其次是亚洲和太平洋地区的国家和经济体，在全球占比为 21.8%，具体如图 1-3 所示。

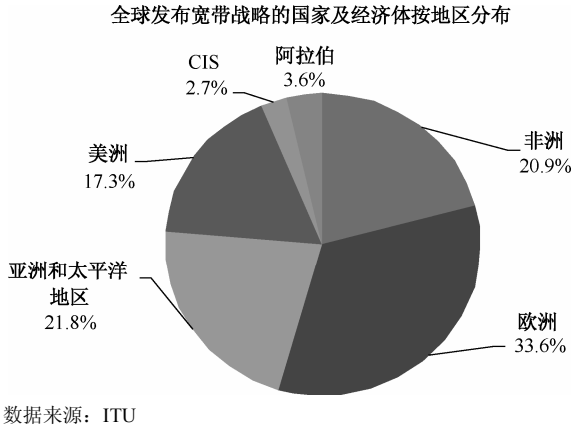



图 1-3　全球发布宽带战略的国家及经济体按地区分布（截止到 2012 年 2 月）

世界各国宽带战略主要目标包括：

① 提出网络建设、速率等目标（Available）；

② 实现所有人能够接入到宽带（Accessable、Affordable），提高覆盖水平；

③ 通过宽带应用实现社会、经济发展目标。

各国宽带战略的重点集中在三大方面。

#### （1）加快建设超高速宽带基础设施

提高基础设施能力是宽带战略最核心的宗旨。纵观全球多国出台的发展战略，各国宽带战略的最主要目标是根据各国的经济发展、现有宽带设施现状及宽带需求，提出高速国家宽带基础设施建设目标。

全球宽带领先的日韩：100Mbps 服务已经普及，计划在今后 2～5 年内提供 1Gbps 的速率，新加坡和日本还希望超高速覆盖到 90%以上的家庭。

宽带较发达的西欧和北欧地区：基本已经实现宽带覆盖，国家宽带发展目标是未来 5 年左右提供 25～100Mbps 的速率，覆盖 75%～100%的家庭。美国目前三挡

（256Kbps～2Mbps、2～10Mbps、10Mbps 以上）用户占比相当，远期目标为 100Mbps 覆盖 1 亿个家庭。

很多发展中国家也提出适合国情的宽带提速计划：印度计划 2014 年大城市家庭实现 10Mbps 接入、中小城市家庭为 4Mbps、城镇和农村地区为 2Mbps。

（2）缩小数字鸿沟，实现宽带普遍服务

各国政府不断采取各种新的举措，促进宽带普遍服务。很多发达国家的目标是在全国范围内提供宽带服务。发展中国家由于宽带普及率比较低，因此根据各国的具体国情制定了相应的宽带覆盖目标，提高偏远地区及农村的宽带覆盖水平。

目前全球已有 20%以上的国家开始实施宽带普遍服务，联合国建议 2015 年所有国家在其普遍服务定义中纳入宽带业务。加拿大在“宽带加拿大：连接乡村居民”计划中，将 2.25 亿美元投入农村宽带基础设施，向提供宽带接入设施的申请者提供一次性的国家资金支持。2010 年巴西政府正式启动《全国宽带计划》，目标是到 2014 年使宽带覆盖 4000 个以前没有覆盖到的中小城市，为 4 千万家庭提供 1Mbps 或更高速率的宽带接入，将宽带人口普及率提高至 68%，同时将月租费降至 15～35 雷亚尔，使普通民众都能承受。在农村地区的光纤网发展方面，印度将通过普遍服务基金投入 41.8 亿美元，“甘地农村就业保障计划”将投入 30.9 亿美元。

（3）普及深化宽带业务应用，服务经济社会发展转型

各国将深化宽带在经济、社会发展中的应用作为重要目标，发展基于宽带的新兴服务业、文化产业，提升个人、中小企业的宽带应用水平。

美国大力推进宽带在医疗、教育、能源、经济、政府执行力与公民参与、公共安全与国家安全等方面的应用，以实现国家目标。欧盟提出到 2015 年，互联网的应用率从 60%上升到 75%，通过网络购物的人数比例达到 50%，33%的中小企业开展电子商务。另外，欧盟委员会还启动了欧洲未来 5 年电子政务管理行动计划，计划中提出 40 项具体措施，帮助公民和企业在网上完成一系列工作，如公司商业登记注册、申请社会福利或医疗保险、大学生登记注册及企业投标等。在发展中国家，古巴、秘鲁、智利和阿根廷，实施了诸如“大学互联网络”等计划，纷纷建立起“虚拟大学”，推动高等教育的电子化和网络化发展。

### 2. 宽带战略实施进展

韩国、日本、芬兰、瑞典等一些战略部署较早的国家阶段目标已经实现，如瑞典提出的 2015 年 40%的家庭和企业至少接入 100Mbps 的宽带阶段性目标，已经提前 4 年实现，韩国早在 2007 年就普及了 100Mbps 宽带网络，日本“e-Japan”计划也已提前实现。

大多数国家已经进入宽带战略的实施阶段。

① 美国：72 亿美元政府宽带资金大部分分配到位，建设计划将在 2013 年 9 月完成。

② 澳大利亚：NBN 公司 2011 年 9 月公司已经完成了第一阶段的计划，在澳大利亚本土实现 5 个地区的光纤用户覆盖，目前第二阶段的计划正在进行中。同时，新的计划和激励政策仍在不断推出。

③ 欧盟：2011 年 10 月推出总额 500 亿欧元的大规模投资计划，用于发展交通、能源和宽带网络，以确保欧盟的未来发展和就业增长。

④ 英国：政府共拨款 10 亿英镑的宽带计划也正在逐步落实。

在目前面临挑战的经济环境中，宽带设施和服务将提升国家竞争力，促进社会经济的增长，增加就业机会。无论是对于全球发达国家还是发展中国家，扩大宽带接入设施和服务都将是国家的重要发展战略。

### 3. 国外超高速宽带应用分析

宽带信息技术的发展蕴涵着巨大的经济增长潜能，能产生诸如支持更高级网络服务、更智能公用事业服务、远程办公等一系列诱导效应，创造出新的经济增长点，进而刺激经济强劲增长。高速率宽带网络可支持如下几个方面的应用：

① 提供各种高质量、互动的带宽应用，如视频会议、家庭视频监控、流媒体和 HDTV 等；

② 促进信息技术在传统产业的应用，如电子政务、电子商务、电子学习等宽带服务。

目前全球领先国家（如日韩）的超高速宽带网络致力于帮助建立一个融合的、无所不在的网络，让用户可以随时随地享受宽带生活。

（1）韩国

韩国的宽带应用发展目标是建立无所不在的社会，运用 IT 技术为民众创造食、衣、住、行、体育、娱乐等各方面无所不在的便利生活服务，韩国政府重点发展的几大宽带应用为智能交通、智能城市、数字家庭、安全应急信息系统等。韩国政府还针对公共部门推出极为低价的网络服务，并针对学校提供免费网络，加快了社会信息化的步伐，提高了科技教育水平。

目前宽带已经成为韩国人生活的一部分，可通过网络解决生活中的难题，用户从被动式使用 Internet 获取信息向交互式业务发展，如网上选举、在线零售、网络游戏、电子教育、手机遥控家用电器等。目前韩国有近四分之一的零售业务都是通过网络实现的，网上银行和网上炒股更是十分普遍。韩国在线游戏服务也发展非常火爆，韩国是世界上 PC 游戏人均花费最高的国家，韩国网游业每年的年度收入增加 9.7%，2016 年将达到 50 亿美元。

（2）日本

日本计划用 ICT 来改变整个社会的形态，构建一个可提供各种信息化应用的大平台，生活中的各类信息应用能够以较低的成本和较高的速度进行开发部署。i-Japan 战略的三大应用领域的总体发展目标如下。

① 电子政府：推动依托数字技术的“新型行政改革”，跨越式地提升便利性，到 2015 年实现政府业务的简洁高效化、标准化及“可视化”。

② 电子医疗：到 2015 年，数字技术与信息将对解决源于人口老龄化、医生数量不足或地区不平衡等的各种问题，做出重要的贡献，医疗品质进一步提高。

③ 电子教育：到 2015 年，幼儿园、保育院、中小学及大学的人才培养，要基本实现信息化。主要内容包括：推进数字技术的应用，实现双向教学；提高学生使用数字信息的能力等。

另外，日本政府还认识到，目前已进入到将各种信息和业务通过互联网提供的“云计算”时代。政府希望，通过执行“i-Japan”战略，开拓支持日本中长期经济发展的新产业，要大力发展以绿色信息技术为代表的环境技术和智能交通系统等重大项目。

### 1.1.3 全球宽带发展模式

宽带经过多年发展，大多数国家已形成以企业投资和市场调节机制为主导的发展模式。但仅靠企业投资和市场调节机制，还不能完全实现国家宽带发展目标。各国普遍采取注入公共资金等方式，从国家层面推动宽带发展。

从政府公共资金介入方式看，宽带发展模式主要有四类：政府直接投资组建公司模式、PPP（Public-Private Partnership，公私合营）模式、PFI（Private Finance Initiative，政府购买服务）模式和政府补助模式。

（1）政府投资组建公司：介入程度最深

这种模式是政府投资组建一个公司，由该公司负责建设新的全国性宽带网络。这种模式是政府介入程度最深的一种模式，也是一种政府推动宽带发展最直接和力度最大的一种模式，还是一种公共资金注入比例最高的模式。这种模式最典型的例子是澳大利亚，还有巴西、卡塔尔、卢旺达等国。

采用这种模式的国家通常没有全国性的宽带网络，或者宽带网络发展明显滞后而国家发展宽带的决心又非常大，希望大幅提升本国宽带网络能力。澳大利亚在出台宽带发展战略之前，澳大利亚宽带发展明显滞后于其他发达国家，尤其是在光网络建设方面，网速慢、收费高。造成这一局面的原因主要有两个：其一，澳大利亚不同届政府对发展宽带政策不一致，导致运营商只有放缓宽带建设步伐来应对政策

风险；其二，澳大利亚地广人稀，宽带网络建设成本高，运营商出于盈利方面的考虑，对宽带建设投资有限。澳大利亚的这种宽带网络现状已经在一定程度上限制了国家的经济活力。因此，澳大利亚将宽带发展目标定得非常高，到 2020 年采用光纤连接 93%的家庭、学校和工作场所，最高传输速率超过 1Gbps。为达到国家的宽带战略目标，并考虑到澳大利亚特殊的地理条件，澳大利亚政府决定采用国家投资组建公司的方式，建设新的全国性的光纤宽带网络。

在这种模式下，政府虽然具有很高的控制权，但并不意味着政府调控完全取代市场调节机制。政府投资主要用来建设全国性的骨干网络，接入网络建设仍以企业为主，市场机制在接入网络建设和运营方面发挥主要调节作用。运营商通过批发网络带宽的方式获得国家建设的骨干网络的使用权。另外，政府为了保证市场调节机制的主导作用，通常会设立政府投资的退出机制。澳大利亚政府规定，将在网络建成并运营 5 年后，出售持有的多数股份，恢复骨干网络领域市场调节机制的主导作用。

这种模式有利于推动网络开放政策的实施和公平竞争环境的营造。由于骨干网络是国家投资建设的，在实施网络开放上的障碍就比企业建设骨干网络要少很多。另外，由于国家组建的公司与接入网络运营商没有太多利益关系，所以也很容易营造一个对所有接入网络运营商来说都公平的竞争环境。

这种模式最大的缺点是公共资金投资巨大。澳大利亚发展宽带政府投入资金为 275 亿澳元，远远高出采用其他模式的国家和地区。过高的投资很容易给政府财政造成巨大的压力。

（2）PPP 模式：资金、风险、技术、经验分担

PPP 模式是政府和企业共同出资建设宽带网络的一种发展模式。与政府组建公司不同的是，PPP 模式更强调政府和企业共同行使决策权、共享技术、共同分担运营风险。另外，PPP 模式下，政府投入的公共资金可通过股权获得收益。PPP 模式比政府投资组建公司方式投资小，适应性强，又能和企业共担风险等。因此，PPP 模式被越来越多的国家采纳，包括欧洲大多数国家。

各国采用 PPP 模式发展宽带主要是为了实现宽带普遍服务。芬兰制定的宽带发展战略中，提出的普遍服务目标是到 2015 年距离 100Mbps 光纤或电缆低于 2 公里的宽带网络人口覆盖率超过 99%。若仅靠企业投资和市场调节机制，2015 年只能实现 94%的覆盖目标。另外，5%的偏远地区宽带网络覆盖需要注入公共资金才能实现。为保证普遍服务的实现及公共资金的更有效利用，芬兰政府明确规定，宽带网络建设中，只有在 100%企业投资财务评价不可行的情况下，才能投入公共资金，并采用 PPP 模式。

PPP 模式下，市场调节机制起主导作用。采用 PPP 模式的国家一般会对公共资金占总投资比重进行限制。芬兰政府提出，在采用 PPP 模式投资建设宽带网络时，

公共资金占比不得超过 1/3，欧盟和市政投资占另外的 1/3，最后 1/3 投资来自企业。西班牙政府规定，政府公共资金投入 8400 万欧元，其中 3100 万属于欧盟构造基金（structural funds），5300 万为无息的公共信贷。运营商投资 2.8 亿欧元。

（3）PFI 模式：主要用于公共应用领域

PFI 模式是政府向企业提出宽带应用服务需求，企业负责建设，最后政府购买企业的宽带服务的一种模式。通过这种方式，政府变相地给予企业资助。与前两种方式最大的差异就是政府的角色不同。前两种宽带发展模式中，政府扮演的是宽带网络建设者的角色，而 PFI 模式中政府扮演的是宽带应用服务购买者的角色。

PFI 模式主要用于宽带应用领域。巴西被认为是 PFI 模式最成功的应用案例。巴西政府通过 PFI 模式，重点资助宽带在政府、教育和公共接入等领域的应用。企业负责敷设宽带接入点，建成后政府全部购入，然后向政府部门、公立学校、图书馆、公众提供免费的宽带接入服务。

欧洲一些国家还将 PFI 模式用于偏远地区的宽带接入服务，如荷兰和意大利。在偏远地区建设宽带网络投资回报率低，运营商投资积极性差，但这些地区对宽带的需求正在日益增长。鉴于此，在这些地区，政府采用 PFI 模式发展宽带服务。

归纳起来，PFI 模式在提升宽带业务应用水平、消除数字鸿沟及刺激经济增长等方面发挥着不可磨灭的作用。

（4）补助模式：企业投资的有效补充

补助模式也是政府向企业投入一笔资金。与政府组建公司和 PPP 模式不同的是，补助模式政府不要求企业的回报，也不参与企业的决策。大多数国家在从国家层面推动宽带发展时，都或多或少地采用了补助模式，其中以补助模式为主要宽带发展模式的有美国、日本等国。

补助模式也主要用于宽带普遍服务。以英国 BT 为例，BT 一直致力于建设光纤网络，但仅靠 BT 自身投资，到 2015 年只能实现 2/3 的家庭光纤宽带网络覆盖，与英国政府要求的 100%家庭覆盖还有很大差距。

补助模式强调的是公共资金是企业投资的有效补充，而不是取代企业投资。

虽然政府的补助是无偿的，但政府通常要求接受政府补助的企业开放网络基础设施，即竞争者也可以平等地不受歧视地接入其网络。

通过前面对四种宽带发展模式的分析及主要国家宽带发展模式的研究，我们发现以下几点。

① 政府公共资金介入以不取代企业投资和市场调节机制为限。政府介入程度最深的政府投资组建公司的宽带发展模式也仅仅是在局部（骨干网）政府调控超过市场调节机制，并制定相应的公共资金退出机制以保证市场机制发挥主导作用。PPP 模式更是通过限制公共资金出资比例来控制政府调控的影响程度。PFI 模式和补助

模式都通过间接方式调控宽带发展。

② 根据本国发展需要确定宽带发展模式，组合宽带发展模式。各种模式各有优缺点和适用范围，单一模式不能满足各国宽带的发展需要。各国普遍采取多种宽带发展模式并行的方式，如欧洲大部分国家采用了 PPP、PFI 和补助模式。

③ 选择经济、合理的宽带发展模式。各国在制定宽带发展目标和发展模式时，都站在整个国家的角度，考虑宽带发展对经济和社会的长期回报，核算宽带对整个国家带来的直接和间接收益/效果、产生的直接和间接费用，对宽带投资（包括国家和企业投资）进行经济评价，在此基础上制定经济、合理的宽带发展目标和发展模式。

## 1.1.4　国外宽带发展扶持政策

为了打造包含“供给”和“需求”双方面的宽带生态系统，国外政府在宽带发展中正在承担越来越重要的角色。政府通过适当的市场监管、普遍服务扩展、灵活的许可制度、直接对网络基础设施进行投资、提供更多的频谱、清除网络建设与使用瓶颈、采用有利于市场的税收政策等支持宽带网与业务（特别是在一些不具备经济可行性的地区）的“供给”。与此同时，政府也在靠提高人们对宽带的认识与技能、对特定用户进行补贴、推进更多的公共服务来刺激宽带的需求与使用。

### 1.“供给”：提升宽带网络建设的主要政策

在提升宽带网络建设方面，政府的工作主要有三个。

① 营造公平的竞争环境。

实践证明，有效的竞争更能促进宽带的发展和提高网络建设和使用效率。竞争对降低资费、提高服务质量至关重要。因此，政府应把创造公平竞争环境的政策放在优先位置。

② 鼓励企业投资。

一方面，宽带过去的发展已经证明企业投资在推动宽带发展中发挥主导作用；另一方面，政府投资成本高，资金有限，完全靠政府投资发展宽带不可行。因此，政府必须考虑如何引导和鼓励将企业投资更多地投向宽带。

③ 建立宽带普遍服务机制。

仅靠市场调节投资和宽带网络建设是不够的，尤其是在地理条件差、人烟稀少的地区。由于在这些地区建设宽带网络投资回报率低，企业投资积极性差。因此，政府应对这些地区宽带建设施加干涉，以确保宽带普遍服务的实现。

#### （1）营造公平竞争环境：网络接入开放

各国在营造公平竞争环境方面的政策主要是网络接入开放政策。宽带基础设施

应实现开放接入是目前在监管方面达成的一个共识。宽带网络所需要的投资规模和范围容易导致产生主导运营商，如果不开放接入宽带基础设施，很容易形成整个宽带市场的垄断，不利于营造公共竞争的发展环境。

各国实现宽带基础设施网络开放接入的方式各异。澳大利亚是政府投资组建公司负责建设一张新的全国性的宽带骨干网，向所有宽带服务提供商采取平等、非歧视的开放措施。新加坡和英国则将宽带网络进行功能拆分。

目前普遍认为，宽带网络基础设施层（物理层、数据链路层和网络层）需要开放接入。基础设施层因具有不可复制性而独具的重要性，如在基础设施层实施可确保公平、透明和开放接入的监管，并有利于推动宽带整体的公平竞争。对传输层是否需要开放存有争议。对应用服务层（会话层、表示层和应用层）很少认为需要开放接入。

（2）鼓励企业投资的政策

① 提供低息贷款。

低息贷款能够降低企业投资的融资成本，引导企业资金投向宽带领域。日本政府要求日本开发银行向本国电信运营商提供宽带接入服务开展上的低息贷款。韩国政府为了发展农村地区宽带网络，曾向 KT 提供 7700 亿美元的低息贷款。

② 对与宽带相关的产业进行减免税，加快设备折旧。

一些国家在探讨对宽带实行减税，来刺激企业对宽带投资。葡萄牙政府准备通过税收减免等政策刺激宽带建设。印度政府为了使宽带价格更加便宜，监管机构要求进口设备免税和加快进行设备折旧。日本政府向宽带接入运营商提供包括企业的税收赎回及加速固定资产的折旧及摊销等在内的税收优惠政策。

③ 为无线宽带提供频谱。

随着业务不断向更强大、无所不在和无缝宽带业务演进，无线宽带频谱需求日益增加。为企业提供所需的无线频谱资源，也能激励企业对无线宽带领域的投资。越来越多的国家开始对本国的宽带无线频谱进行规划。首先，测算未来频谱需求，然后通过加速无效或低效频谱释放、频谱共享等措施为企业腾出更多频段，还加紧对“数字红利”和 White Space 的研究，为企业寻找更优质的无线宽带频段。

④ 开放路权。

大部分的有线网络基础设施成本是土木工程。开放包括道路、铁路、管道、电力输送线路等公共基础设施路权，能够显著降低土木工程费用，进而极大地激发企业对宽带网络的投资。开放路权的方式主要有三种：一是将路权接入费用降低到宽带网络建设者可接受的范围内；二是简化路权接入法律程序；三是向宽带网络建设者免费提供国家拥有控制权的路权基础设施。

（3）普遍服务机制

在过去，大多数国家都将普遍服务定义为优先满足固定电话服务。目前国外一些国家通过创建宽带普遍服务基金或修改之前的普遍服务基金，将宽带纳入普遍服务范畴内。通过普遍服务基金这种长效保障机制，来支持农村和欠发达地区的宽带普遍服务建设。这笔钱从运营商的业务收入中按照一定的比例征收，由监管机构向为高成本地区（农村、边远地区等）提供服务的运营商进行再分配，以及补助低收入人群、学校图书等的连网项目。

以美国为例，美国将建立“连接美国基金”（CAF，Connect America Fund），以实现普通大众负担得起的实际下载速度至少为 4Mbps 的宽带服务。FCC 计划在未来 10 年里，普遍服务基金（USF，Universal Service Fund）从语音时代的 80 亿增长到 155 亿美元，以支持宽带建设。如果国会希望加速实现宽带普遍服务，可在未来 2～3 年内每年提供几十亿美元的公共基金。

### 2.“需求”：提升宽带需求与应用主要政策

提升宽带需求和应用的相关政策，与本国文化、经济背景及宽带发展程度关系密切，因此，各国在具体政策上有很大差异。到目前为止，提升宽带需求和应用方面的政策多来自发达国家，相类似的政策对发展中国家的可借鉴性也要根据实际情况而定。

当前主要的提升宽带需求和应用的政策概括起来可以分为三类。

（1）网络侧的宽带政策

- 用宽带连接学校；
- 政府优先使用；
- 用普遍服务基金把网络接入到欠服务社区；
- 建立社区接入中心；
- 把宽带纳入普遍服务。

（2）业务和应用侧的宽带政策

- 政府引导培育应用；
- 提供电子政务应用；
- 促进数字内容发展，支持本地内容；
- 推进医疗、教育、农业等方面的宽带应用。

（3）用户侧的宽带政策

- 向教育机构提供低成本用户终端；

- 进行数字化扫盲；
- 使宽带终端价格可承受；
- 监测服务质量；
- 打造电子商务安全交易环境；
- 对中小企业进行培训。

分析各国宽带需求和应用提升政策及所要解决的主要需求问题，发现宽带需求问题主要有三类。

① 宽带服务更深层次的普及问题。

如果一个国家中对宽带服务接受能力强的潜在消费群体已经基本转化为实际的宽带服务消费者，那这个国家在提升宽带需求方面面临的主要问题是如何向不了解宽带和对宽带兴趣不足的潜在消费群体普及宽带。针对该问题各国普遍采取的措施有：对潜在人群的宽带知识普及，提高数字素养；鼓励宽带在教育和中小企业中的应用。

② 提供可支付得起的宽带服务。

如果一个国家的宽带资费对大多数人来说较贵，那该国在提升宽带需求和应用方面所应做的工作就是对终端和资费的补贴。

③ 宽带应用吸引力问题。

如果一国宽带已经发展到较高水平，那该国在提升宽带需求和应用方面则应侧重跨宽带应用水平的提升和创新力度的增强。

另外，政府对提升宽带应用的一些扶持政策也具有一般特性，可以借鉴。各国普遍采取的扶持政策主要有以下两个。

① 政府建设基于宽带的公共服务、教育、医疗等平台。

为了推动宽带应用，一些国家的政府出资建设公共服务、教育、医疗平台。例如 2011 年 10 月获批的 500 亿欧元“连接欧洲基础设施”项目，92 亿欧元的宽带资金中就包括资助电子身份证、电子采购、电子保健记录、欧洲数字图书馆、电子司法和海关相关服务所需的基础设施平台的建设。

② 解决用户接入费、终端与知识技能等问题。

国外的普遍服务基金中有一部分是用于贫困人口的接入补贴，过去是对电话业务进行补贴，现在逐步转到对宽带业务的补贴上。

用户终端是宽带普遍服务得以顺利开展的基础。目前，宽带终端除了计算机外，还有移动智能手机、上网本等新设备。若实现宽带普遍服务，需解决贫困人口或需要财政补贴的机构（如中小学）如何获得终端的问题。除了建设网络、配置终端外，还需要对用户意识进行培养，进行 ICT 技能开发，以及“数字扫盲”。例如，美国成立了一个国家数字技能小组，组织年轻人和成年人进行培训，教授数字技能，以缩小受教育程度上的差距。

E-rate 项目是美国针对学校、图书馆的普遍服务项目。按照宽带计划的建议，

FCC 需要更新和提升 E-rate 项目，目前美国 97%的学校和几乎所有的公共图书馆都有基本的互联网接入，但速率慢。FCC 最新通过的 E-rate 政策包括：① 高速光纤——对学校的光纤接入进行资金支持，学校可以选择多种方式得到光纤接入，包括通过现有的地区和本地网，或利用当地未使用的光纤线路进行的高速接入；② 学校热点——学校可以建设热点，向周边社区提供互联网接入，以方便学生回家使用，并带动周边发展；③ 学习随身行（Learning On-the-Go）——FCC 试点把上网本、平板电脑等无线终端用于课堂的内外，使学生不用在固定的地点进行学习。

### 3.“国家投入”：给予宽带发展财税政策支持

国外政府普遍对发展宽带给予财税支持，各国支持力度、方式和领域不尽相同。

（1）国家投入力度

各国根据宽带发展目标、当前宽带发展水平、政府的财力、拟采取的扶持方式等，对发展宽带的投入金额和力度不同，具体如图 1-4 所示。

从投入金额上来看，澳大利亚投入的金额最大，为 275 亿澳元。

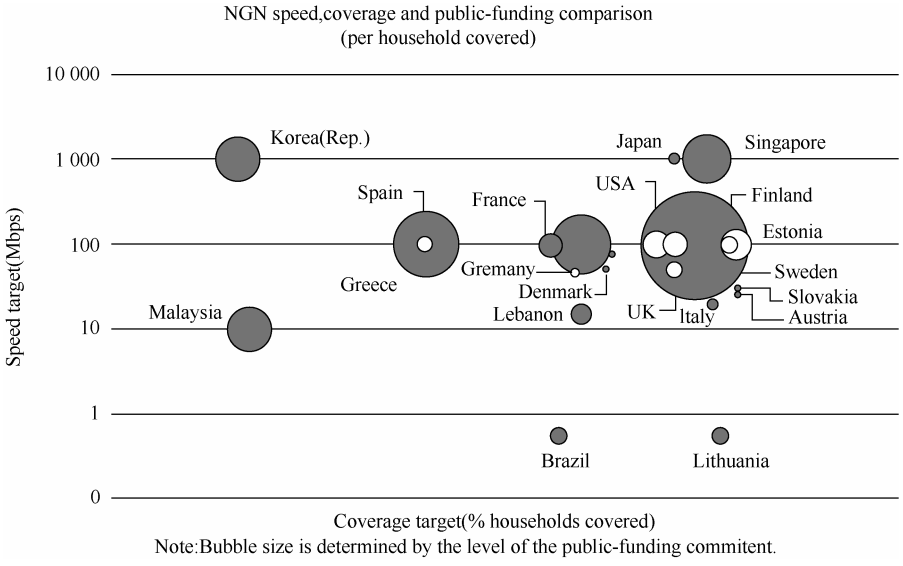



图 1-4　国家投入力度对比

从平均到每公民的公共投资上来看，新西兰的投入力度最大，为 200 美元/公民；其次是澳大利亚，为 160 美元/公民，具体如图 1-5 所示。

（2）扶持方式

各国政府普遍采取多种扶持方式支持宽带发展，扶持方式可分为两类：直接扶

持和间接扶持。

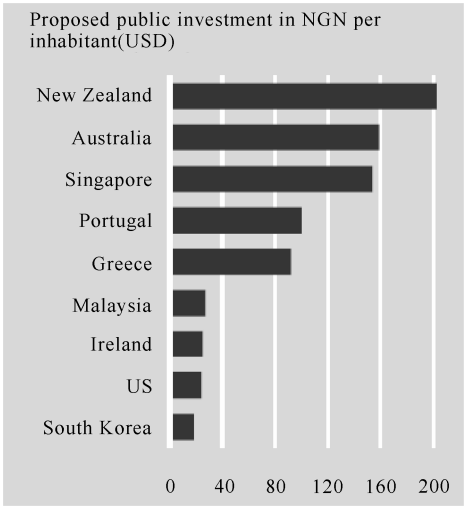



图 1-5　平均到每个公民的公共投资

1）直接扶持

① 一次性资金投入（见表 1-1）。

表 1-1　各国一次性资金投入情况

| | |
|---|---|
| 美国 | 经济复苏计划中的 72 亿美元宽带基金，其中一部分是直接拨款（grants） |
| 澳大利亚 | 直接投资 275 亿澳元 |
| 韩国 | 2009 年 2 月韩国政府宣布中央政府将直接投资 1.3 万亿韩元用于宽带建设 |
| 巴西 | 巴西政府宣布向 PNBL（《全国宽带计划》）投资 110 亿雷亚尔（约 61 亿美元），其中 2011 年起 4 年内向前国有电信运营商 Telebras 投资 32.2 亿雷亚尔（20.3 亿美元） |
| 英国 | 政府计划直接出资 8.3 亿英镑 |
| 芬兰 | 政府将直接出资 6 700 万欧元 |

② 为宽带发展改革现有普遍服务机制。

在过去，大多数国家都将普遍服务定义为优先满足固定电话服务。目前国外一些国家通过创建宽带普遍服务基金或修改之前的普遍服务基金，将宽带纳入普遍服务范畴内。通过普遍服务基金这种长效保障机制来支持农村和欠发达地区的宽带普遍服务建设。

表 1-2　改革机制情况

| | |
|---|---|
| 美国 | 将建立“连接美国基金”（CAF，Connect America Fund），以实现普通大众负担得起的实际下载速度至少为 4Mbps 的宽带服务。FCC 计划在未来 10 年里，普遍服务基金（USF，Universal Service Fund）从语音时代的 80 亿增长到 155 亿美元，以支持宽带建设 |
| 巴西 | 国家电信投资基金 Funntel 将提供 17.5 亿雷亚尔用于启动宽带计划的相关研究开发项目 |

续表

| | |
|---|---|
| 韩国 | 2009 年 2 月韩国政府宣布中央政府将直接投资 1.3 万亿韩元用于宽带建设 |
| 巴西 | 巴西政府宣布向 PNBL（《全国宽带计划》）投资 110 亿雷亚尔（约 61 亿美元），其中 2011 年起 4 年内向前国有电信运营商 Telebras 投资 32.2 亿雷亚尔（20.3 亿美元） |

2）间接扶持

① 减免税收和加速设备折旧（见表 1-3）。

表 1-3　减免税收和加速设备折旧情况

| | |
|---|---|
| 日本 | 政府向宽带接入运营商提供税收优惠，包括企业的税收赎回及对固定资产的折旧及摊销税收优惠 |
| 印度 | 免除 ISP（互联网接入服务商）最初 5 年的业务收入税费，其原来的征税比例是 ISP 所提供业务收入的 8%；<br>要求进口设备免税 |
| 葡萄牙 | 政府承诺颁布法律，通过税收减免政策刺激宽带发展 |
| 巴西 | 分为免税州和非免税州，免税的州以 29.80 雷亚尔/月、非免税州以 35 雷亚尔（22 美元）/月提供不低于 1Mbps 高速因特网接入 |
| 英国 | 宽带网络建设资金的 2/3 来自私营企业，首年资本免税 |

② 低息贷款（见表 1-4）。

表 1-4　低息贷款情况

| | |
|---|---|
| 日本 | 提供宽带接入提供上的债务担保和由日本开发银行的低利率融资 |
| 韩国 | 为了向农村地区建设宽带网络，政府曾经向 KT（韩国电信）提供了 7700 万美元的低息贷款 |
| 巴西 | 国家开发银行 BNDES 将向 Telebras 和其他运营商提供 75 亿雷亚尔低息贷款 |

③ 扶持领域。

各国对宽带的扶持领域可分为“供给”和“需求”两个领域。“供给”主要指宽带基础设施建设，“需求”主要指激发用户对宽带的应用。各国的宽带扶持政策主要还是在“供给”领域。

a.“供给”。

侧重在农村等偏远地区的宽带网络建设（见表 1-5）。

表 1-5　“供给”领域

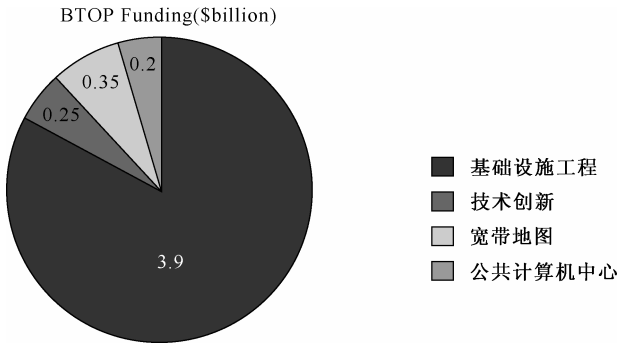
| | |
|---|---|
| 美国 | 72 亿美元的宽带基金主要用于扩大宽带连接的覆盖范围、提高宽带的普及率 |
| 欧盟 | 重点投入 10 亿欧元，用于发展欧盟成员国偏远地区的互联网基础设施 |
| 英国 | 政府投资的“下一代基金”主要用于英国三分之一（相对偏远地区）的下一代网络建设 |
| 印度 | 通过普遍服务仅投入 41.8 亿美元，用于农村地区的光纤网络建设 |

b.“需求”（见表 1-6）

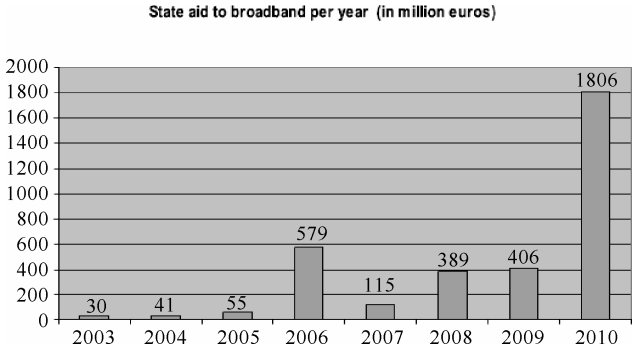
表 1-6 “需求”领域

| | |
|---|---|
| 美国 | 将为图书馆、大学和其他公共单位的计算机中心及培训互联网使用方法的项目提供资金资助，另外还包括 3.5 亿美元的宽带地图专款 |
| 英国 | 出资 4.8 亿美元为低收入家庭提供宽带补贴 |

表 1-7 典型国家政府对宽带发展的财税政策

| | |
|---|---|
| 美国 | 经济复苏计划中的 72 亿美元宽带基金。<br>72 亿美元包括：直接拨款（grants）、贷款（loans）和贷款担保（loan guarantees）。其中的 47 亿美元由美国商务部、国家电信和信息管理局（NTIA）提供（通过 BTOP），其余的 25 亿美元由农业部农村公用事业服务处（RUS）提供（通过 BIP）。这些资金将全部按照经济复苏计划的要求拨付，用以扩大宽带连接的覆盖范围，提高宽带的普及率。<br>美国商务部的项目一般采取“国拨+配套”的方式。重点关注连接图书馆、大学和公共安全机构等的“中间英里（middle mile）”项目；此外，它也将为图书馆、大学和其他公共单位的计算机中心及培训互联网使用方法的项目提供资金资助，另外还包括 3.5 亿美元的宽带地图专款。资助的项目有 200 多个，大部分为网络建设，具体分配如下图所示。<br>  <br><br>网络项目例如：环乔治亚北部山区的 260 英里光纤环路项目（国拨 3350 万、North Georgia Network Cooperative 公司配套 8800 万）、缅因州山区的光纤网络等。计算机中心项目主要是资助学校和图书馆。宽带的使用主要是促进计算机扫盲和互联网使用。宽带地图则是建设基于地理信息系统的宽带监测平台。<br>美国农业部的项目既包括“最后一英里”，又包括“中间一英里”，重点关注为家庭、企业和其他终端用户提供“最后一英里”互联网连接的项目，主要解决农村和边远地区宽带覆盖，如资助阿拉斯加 Rivada Sea Lion 公司向欠服务的地区提供 4G 服务（2530 万美元国拨资金加 640 万美元撬动基金），资助夏威夷大岛的 Big Island Broadband/Aloha Broadband 向北部岛屿上的 600 个居民和企业提供宽带服务（拨款 10 万，配套基金 8.7 万） |
| | 宽带普遍基金：FCC 建立“连接美国基金”（CAF，Connect America Fund），以实现普通大众负担得起的实际下载速度至少为 4Mbps 的宽带服务。把目前用于补贴高成本地区电话服务的 45 亿美元改为补贴宽带服务。FCC 计划在未来 10 年里，普遍服务基金从语音时代的 80 亿美元增长到 155 亿美元，以支持宽带建设。此外还要成立创建移动基金，提供有针对性的资金支持，确保美国任何一个州的 3G 无线网络覆盖达到普遍服务的最低要求 |

续表

| | |
|---|---|
| 欧盟 | 2008 年资助 10 亿美元，用于实现 2010 年 2Mbps 高速 Internet 覆盖 100%，资助对象主要在郊区农村（如“白点（无服务）”和“灰点（服务欠缺）”地区）；<br>欧盟 2003 年以来逐年对成员国进行宽带国家援助。在 2010 年，欧盟共批准了 18 亿欧元的宽带国家援助项目，是 2009 年获批金额的 4 倍多，如下所示。<br>  <br><br>欧盟委员会 2011 年 10 月 19 日宣布，欧盟将推出总额 500 亿欧元的大规模投资计划，用于发展交通、能源和宽带网络，以确保欧盟的未来发展和就业增长。500 亿欧元中有 92 亿欧元用于建设欧洲的高速、超高速宽带网络，并改善数字服务。这一项目将吸引数额更大的私人和公共资金投资基础设施建设与服务。欧盟委员会预计每投资 1 欧元就将吸引 6～15 欧元。92 亿欧元的宽带启动资金预计将吸引 500～1000 亿欧元的投资到宽带网的建设之中 |
| 日本 | 2008—2009 年期间，日本政府共在智能交通系统、改进 ICT 网络设施、培训、农村地区宽带建设上投资 371 亿日元。<br>日本政府向宽带接入运营商提供税收优惠，包括企业的税收赎回及对固定资产的折旧及摊销税收优惠，它还提供宽带接入提供上的债务担保和由日本开发银行的低利率融资 |
| 韩国 | 2009 年 2 月韩国政府宣布 2012 年提供 1Gbps 的宽带计划，此计划在未来 5 年耗资 34.1 万亿韩元，中央政府将投资 1.3 万亿韩元，余下的由私营运营商提供。此前，在 2006 年政府就宣布向 FTTH、光纤 LAN、FHC 投资 26.6 万亿韩元。<br>为了向农村地区建设宽带网络，政府曾经向 KT（韩国电信）提供了 7700 万美元的低息贷款 |
| 巴西 | 巴西政府宣布向 PNBL 投资 110 亿雷亚尔（约 61 亿美元），其中 2011 年起 4 年内向前国有电信运营商 Telebras 投资 32.2 亿雷亚尔（20.3 亿美元）。同时，国家开发银行 BNDES 将向 Telebras 和其他运营商提供 75 亿雷亚尔贷款。此外，巴西国家电信投资基金 Funntel 将提供 17.5 亿雷亚尔，用于启动宽带计划的相关研究开发项目。<br>国有运营商 Telebras 是 PNBL 计划的主要承担者，民营运营商扮演补充角色。2011 年 6 月 30 日，巴西最大的四家民营运营商 Oi、Telesp TLPP4.SA、CTBC 和 Sercomtel 也宣布参与巴西的国家宽带计划，在免税的州以 29.80 雷亚尔/月、非免税州以 35 雷亚尔（22 美元）/月提供不低于 1Mbps 高速因特网接入 |

续表

| | |
|---|---|
| 芬兰 | 2009 年 10 月，政府正式提出将“宽带权”确认为公民基本权利。7 月 1 日起，芬兰把宽带接入权确认为公民基本权利之一，芬兰由此成为世界首个通过立法的形式确认“宽带权”的国家，芬兰成了世界上第一个把宽带接入确认为公民基本权利的国家。根据新规，自 1 日起，无论用户身处何地，芬兰所有网络服务商有义务给他们提供 1Mbps 的宽带上网服务。芬兰通信部表示新法是“政府在地区政策上取得的最重要成绩之一。<br>芬兰政府希望通过私有资本、政府补贴、当地政府基金以及欧盟的投入来实现宽带普遍服务，达到 100Mbps 宽带覆盖 99%的目标，其中联邦政府的补贴不超过 1/3，当地政府及欧盟的支持占 1/3，私有投资至少占 1/3。政府投资大约 1.31 亿美元。<br>芬兰政府称，第一阶段的目标是 2010 年使宽带速率至少达到 1Mbps。为此，芬兰政府将提供三分之一的费用，其余三分之二将来自地方政府、欧盟财政支持及电信运营商。该项目中光纤网络的建设费用约为 2 亿欧元，芬兰政府将提供 6 700 万欧元 |
| 澳大利亚 | 澳大利亚采用政府持股 51%，组建新公司—国家宽带公司（NBN 公司）的方式，建设国家级的宽带网络，然后向其他公司出租宽带服务。澳大利亚国家 NBN 建设投资计划主要包括：NBN 网络计划总资本开支为 359 亿澳元；其中政府投资 275 亿澳元，其他的来源于借债和收益；至少十年之内，政府将拥有 51%的股份，并将负责经营网络；有一个专门的议会委员会监督 8 年施工过程；所用运营商平等使用一切设施。澳大利亚政府表示，NBN 的敷设成本将从最初预计的 430 亿澳元减少约 70 亿澳元，大约为 359 亿澳元。<br>为了支持 NBN 网络的建设，充分利用原有网络资源，减少投资。在长达数日的紧张协商和激烈辩论后，2010 年 11 月底澳大利亚参议院批准了一份至关重要的政府提案，同意拆分 Telstra 的零售业务和批发业务，同时将准许 NBN 公司使用 Telstra 的地下基础设施，且 Telstra 将成为国家宽带网络的用户，此举为国家宽带网工程铺平了道路。Telstra 首席执行官大卫• 托德利已表态愿意与澳大利亚政府合作，支持分拆法案。在未来十年中，政府将支付给 Telstra 138 亿澳元，作为其逐渐退出市场，将基础设施供 NBN 工程使用的补偿 |
| 俄罗斯 | 2010 年 7 月，俄罗斯政府信息技术委员会批准了俄罗斯通信部制定的关于实施建设“2011～2020 信息社会”长期方案的草案。俄罗斯计划在未来 10 年内，每年对该项目投资 100 亿卢布（约 20.6 亿元人民币），投资总额达 1000 亿卢布 |
| 英国 | 宽带网络建设资金 2/3 来自私营企业，首年资本免税。大部分乡村的宽带建设资金来自公共基金。政府计划出资 8.3 亿英镑，其中一部分来自给 BBC 公司用于支付切换到数字电视的基金。8.3 亿英镑中的 5000 万英镑用于偏远地区宽带接入试验，包括北约克郡、赫里福郡、坎布里亚郡高原和岛屿等。2011 年年 11 月，英国政府再拨款 1 亿英镑建设 10 个超高速宽带城市 |

## 1.2 典型国家宽带发展战略

当今世界各国普遍把抢抓宽带数字机遇作为抢占新一轮科技和产业变革制高点的战略支点。当前，宽带正牵引着新一代信息技术产业的蓬勃发展，重塑着制造业和服务业竞争新优势，并成为国家科技资源汇聚和技术创新的战略性关键基础设施。为牢牢抓住数字经济机遇，各国纷纷将建设宽带国家作为优先突破点。例如，美国

2009 年投入 72 亿美元支持宽带发展，欧盟在 2011 年投入 92 亿欧元支持高速宽带网基础设施和公共服务平台建设，英国在先前 5.3 亿英镑的基础上 2011 年再拨款 1 亿英镑用于 10 座城市的“超高速固定和移动宽带网络”建设，巴西 2010 年投入 73 亿美元用于在低收入家庭普及宽带网络，印度 2010 年投入 30.9 亿美元发展农村地区高速宽带网络。据国际电信联盟（ITU）2012 年年底最新统计，全球主要发达国家和 127 个发展中国家已提出和实施了宽带发展国家战略或行动计划，并给予资金和政策支持，其重点是支持超高速网络部署和农村宽带普及，还对提高宽带应用水平与业务创新进行了重点扶持，以期宽带能够更好地带动经济增长。除政府直接投资外，还有 40 多个国家已经建立起宽带普遍服务长效机制。

## 1.2.1　欧盟

### 1. 战略定位

目前，欧盟各成员国的互联网用户已经超过 2.5 亿户，英、德、法、瑞典等成员国的宽带使用率也都排在世界前列，从整个欧盟的范围来看，其宽带使用率已经达到 24.8%，仅次于日、韩和美国。

在全球宽带发展提速的大背景下，欧盟期望能够在自身无线和移动通信发展所具备较大优势的基础之上，将下一轮宽带的发展与移动互联网等紧密结合起来，逐步摆脱在现有互联网发展格局中一直以来欧盟对美国的跟随态势，从而实现欧盟在全球互联网领域对美国的超越，并能够最终奠定欧盟在全球互联网领域的领先地位。

国际金融危机爆发后，欧盟已经把发展信息技术提升到战略高度，将信息技术确立为欧洲实现经济复苏的重要手段。2010 年 3 月欧盟委员会出台《欧洲 2020 战略》，把“欧洲数字化议程”确立为欧盟促进经济增长的七大旗舰计划之一，其目标就是在高速和超高速互联网的基础上，提高信息化对欧洲经济社会的贡献率，到 2013 年实现全民宽带接入，2020 年所有互联网接口的速度达到 30Mbps 以上。欧盟委员会预计电信运营商需要投资 2500 亿欧元（3180 亿美元）实现这一目标。

欧盟宽带战略中尤其重视基于欧盟在移动通信领域的既有优势来发展无线宽带网络。集宽带与无线特点于一身，具备性价比优越、建设周期短、服务提供快速、具备较大灵活性、系统资源可动态分配、系统维护成本低等优点，已经在整个欧盟电信市场中占据着越来越重要的地位。而同时，也几乎是每个欧洲人都拥有自己的一部或几部手机。欧洲已经具备开展无线宽带业务的天然的用户群体和成熟的市场。

### 2. 欧盟宽带发展战略的实现目标

欧盟的《欧洲 2020 战略》，把“欧洲数字化议程”确立为欧盟促进经济增长的

七大旗舰计划之一，其目标就是在高速和超高速互联网的基础上，提高信息化对欧洲经济社会的贡献率。具体说来，在《欧洲 2020 战略》中，欧盟关于宽带战略的发展目标可以分为三个阶段。

第一阶段（到 2013 年），为近期基本目标：到 2012 年年底，在欧盟各成员国内至少发展 1400 万个 FTTH 用户；到 2013 年，实现欧盟范围内的全民宽带接入。

第二阶段（到 2015 年），为中期发展目标：到 2015 年，50%的欧盟公民可以在线购物，20%的公民可以实现跨境网上服务；到 2015 年，互联网的应用率从 60%上升到 75%，而在残疾人中，互联网的应用从 41%上升到 60%；到 2015 年，从没用过互联网的欧盟公民数量从 30%下降到 15%；到 2015 年，至少 50%的欧盟公民可以享受到在线的公共服务。

第三阶段（到 2020 年），为最终实现目标：到 2020 年，所有互联网接口的速率都在 30Mbps 以上，至少一半的欧盟家庭宽带接入速率可以达到 100Mbps；到 2020 年，欧盟成员国每年在 ICT 研发上的投资总额要达到 110 亿欧元。

### 3. 欧盟发展宽带战略的具体举措

为了实现在《欧洲 2020 战略》中所设定的宽带发展战略目标，欧盟希望在联合和协调各个成员国的基础上，放眼整个欧洲，通过鼓励和增加投资、发展无线宽带和合理使用发展基金等具体建议，来促进欧洲的宽带通信发展，从而推动整个欧盟社会的信息化进程。

#### （1）降低宽带投资成本

资金投入是宽带发展的首要保障。欧盟积极鼓励各成员国从国家和地区等不同层面加大对宽带通信发展的投资。同时，欧盟建议在宽带建设和发展的过程中，积极寻求宽带建设和发展投资成本的降低。关于宽带建设和投资成本的降低，欧盟对其各成员国及其各级相关部门的建议如下。

① 通过提高信息透明度和减少信息壁垒及合理调配相关资源等方式，有效利用现有资源及防止重复建设等，来降低和减少投资成本。

② 通过消除相关行政障碍，如新基站等基础建设项目获取权限的层层审批、已有合同在续签方面存在的困难等，来降低宽带建设的投资成本。

#### （2）推进无线宽带发展

由于在无线宽带方面已经发展多年并具备较大优势，因此，欧盟希望借助无线宽带的发展来带动其整个宽带领域的战略发展。频谱是发展无线宽带的重要资源，欧盟正在尝试通过合理分配频谱这种稀缺资源，来建立泛欧的无线宽带与有线宽带相配合的泛在网络。关于无线宽带频谱资源的分配，欧盟的建议如下。

① 欧盟委员会建议欧盟各成员国在 2013 年之前把电视台使用的一部分有价值

的广播频率提供给移动运营商，以支持创建一个欧盟范围的无线宽带服务市场。这一建议是欧盟宽带网改革计划的一部分，要求其 27 个欧盟成员国在 2013 年 1 月之前把 800GHz 频带分配给移动宽带网。

② 在全球宽带提速的背景下，欧盟通过合理分配频谱，增加在频谱资源分配方面的灵活性和竞争性，如鼓励频谱资源的快速应用、允许频谱资源的二次交易等，以期充分发挥稀缺资源的价值。泛欧无线宽带与有线宽带配合的泛在网络不仅将推动整个社会信息化进程，更成为提振经济、增强核心竞争力的手段。

（3）合理使用宽带发展基金

欧盟通过建立 SRD（Structural and Rural Development）基金的形式来支持欧盟范围内宽带通信的建设和发展。2007 年到 2013 年期间，总共计划将 23 亿欧元的 SRD 基金用来投资宽带的建设和发展。关于 SRD 基金有关投资的管理、分配和推广等问题，欧盟给出了如下的建议。

① 在 2011 年，发布宽带投资指南，鼓励和指导各成员国及其相关部门申请和有效使用宽带发展基金和投资。

② 在 2011 年，邀请业内外人士参加基金支持的宽带发展项目，并征询关于宽带发展的相关意见和看法。

③ 重新启动和扩大欧洲宽带门户网站，以提供一个多语言宽带平台。基于该平台，可方便相关宽带发展项目信息和资料的交流及诸如国家援助规则、监管框架执行等问题上的指导等。

## 1.2.2　美国

### 1. 战略定位

美国凭借其在互联网领域的先发优势，从 20 世纪 80 年代至今一直占据着全球信息通信领导者的地位。在全球信息通信技术变革和产业融合转型的关键时期，尤其是在应对全球金融危机的重要关头，美国希望通过发展宽带战略来促进信息通信的技术创新和业务创新，构建新型国家信息基础设施，继续保持其在未来信息社会的技术和产业制高点。

美国发展宽带战略有着良好的基础。美国商务部 2010 年 2 月发布的报告显示，2009 年美国的宽带普及率已经达到 63.2%，比 2007 年提高了 13%，提高幅度比较大。而与之相反的是，美国宽带的性能则比较差，提升速度显得比较缓慢。根据美国电信工会（CWA）的报告显示，美国的宽带接入速率为 5.1Mbps，相比 2007 年 3.5Mbps 的速率仅提高了 1.6Mbps。

并且，在美国不同收入、年龄、种族群体、地域的宽带用户分化严重。年收入

不足 1.5 万美元的家庭宽带普及率最低，为 29.9%；年收入超过 15 万美元的家庭宽带普及率最高，达到 88.7%。18～24 岁年龄组的家庭宽带普及率最高，为 80.8%；55 岁及以上年龄组的家庭宽带普及率最低，为 46%。同时，美国很多郊区及农村的宽带网络基础设施不完善，到 2009 年年底，农村家庭的宽带普及率为 54%，比城市低 12%。

### 2. 战略目标

2009 年 2 月，为了应对金融危机，奥巴马签署美国经济恢复与投资计划（ARRA 2009），其中用于宽带发展的资金达到 72 亿美元。2009 年 4 月，FCC 开始着手制定有关美国宽带发展的战略计划。2010 年 3 月 15 日，美国 FCC 在征询本国公民意见的基础上，FCC 向国会提交《国家宽带发展战略》，实现六大目标。美国最新的宽带战略发展重点是提高基础设施水平、提高速率、扩大覆盖面，最终实现全民共享。这些目标包括。

目标一：到 2010 年保证至少 1 亿美国家庭应能使用平价宽带，实际下载速度至少达 100Mbps，实际上载速度至少达 50Mbps。

目标二：美国应在移动创新上领先世界，在世界所有国家中拥有最快和范围最广的无线网络、每个美国人能够接入得起宽带服务。

目标三：每个美国人都应能获得强大的宽带服务，在选择订购时具备相应的手段和技能。

目标四：每个美国社区都应能获得至少 1Gbps 的宽带服务，从而为学校、医院和政府大楼等机构提供支持。

目标五：为确保美国人民的安全，每个急救者都应能使用全国范围内的无线、互通互操作的宽带公共安全网络。

目标六：为确保美国在清洁能源经济上领先，每个美国人应能使用宽带实时跟踪和管理其能源消耗。

### 3. 战略举措

美国政府计划从四个方面着手，实现六个长期目标，确保宽带生态系统的健康发展。

① 建立竞争机制，通过健康竞争使消费者利益最大化，并在此基础上促进创新和投资。

- 收集、分析、发布每个市场详细的宽带服务价格和竞争情况。
- 要求宽带服务提供商公布其宽带服务的价格和性能等信息，以便消费者能够选择市场上的最佳服务。
- 对竞争条例进行全面评估。

- 释放并分配无牌照使用的额外频谱资源。
- 提高宽带服务在城区的容量和在农村地区的覆盖范围。
- 采取行动，确定如何最好地实现广泛、无缝、具有竞争力的宽带覆盖。
- 改革相关法规，营造具有竞争力和创新性的视频机顶盒市场。
- 充分保护消费者隐私。

② 通过对国有资产进行有效分配及管理，促进宽带基础建设的实施，并降低竞争门槛。

- 在 10 年内，重新获得 500MHz 频谱，并在 5 年内将 300MHz 用于移动用途。
- 鼓励频谱拍卖。
- 确保频谱的分配和使用更加透明。
- 加强对新频谱技术的研究。
- 改进通行权管理，促进美国宽带基础设施的使用。
- 实施“一次挖掘（dig-once）”等政策，促进基础设施的有效建设。
- 为国防部提供超高速宽带连接，为军队开发下一代宽带网络应用。

③ 建立连接美国基金（Connect America Fund），以普及大众能支付得起的、实际下载速度至少为 4Mbps 的宽带和语音服务。

- 建立连接美国基金（Connect America Fund），确保普通大众对宽带网络的普遍访问。
- 创建移动基金，确保任何一个州都能达到 3G 无线网络覆盖的平均水平。
- 改革运营商之间的载波频谱补偿制度。
- 以减轻赋税的方式，设计新的连接美国基金，以缩小宽带鸿沟，并减轻消费者负担。
- 针对低收入家庭，建立确保其能支付得起的宽带服务机制。

④ 完善法律、政策、标准和奖励措施，在政府主要部门最大限度地发挥宽带所带来的好处。

- 卫生保健：通过宽带服务提升卫生保健的质量并降低其价格。
- 教育：通过使用宽带服务，学生能够进行远程教育并获取在线内容，促进公共教育改革。
- 能源和环境：利用宽带技术的创新，减少碳排放、提高能源利用率，从而减轻美国对外国石油的依存度。
- 经济机会：宽带可以提高获取工作和接受培训的机会，支持企业的发展等。
- 政府执行力和公民参与度：宽带可以促进政府服务制度和内部流程操控更加有效，并能改善公民参与的数量和质量。
- 公共和国家安全：宽带通信服务可以使得应急救护人员及时获取相关信息等。

### 1.2.3 日本

日本的宽带接入市场自 2000 年以来快速增长，目前在宽带普及率、接入速度及应用的丰富程度等各个方面均处于全球领先位置。对于日本宽带的快速发展，国家战略一如既往的支持，是一个非常重要的推动因素。

在 2009 年之前，日本政府先后发布了 e-Japan 计划（2001—2005）和“u-Japan”计划（2004—2010）及 IT 新改革战略等。在 2009 年 7 月，日本又推出国家信息化战略《i-Japan 战略 2015》。在该战略中将投资 19 亿美元，到 2015 年实现以光纤（Gb 级）速率快速且简单的网络接入，建设高质量、高稳定性的超高速宽带基础设施。在 2010 年 9 月，日本政府在公布的《新经济发展战略蓝图》中称，将通过推进基础设施建设，力争到 2015 年左右使国内全部约 4900 万户家庭能够利用宽带网络服务。

### 1.2.4 韩国

作为全球宽带普及率最高的国家，韩国重视宽带网络的多元化发展和应用，将其与 IP 有线电话、3G/4G 无线上网和数字电视地面广播的发展紧密结合。

韩国政府在其 2009 年 1 月颁布的《2009—2013 年广播通信网中长期发展计划》中提出，投资 325 亿美元，在 2013 年前实现目前 60%的有线电话 IP 化，普及 VoIP 网络电话。至 2012 年，针对韩国国内 1400 万用户提供 50Mbps～100Mbps 有线上网服务，2012 年后建造超高速宽带网络，提供 1Gbps 有线上网服务，对 4000 万用户提供 1Mbps 的 3G 无线上网服务，2013 年推出 10Mbps 的 3.9/4G 服务。2010 年前除建造 IPTV 之外，将地面电视广播基础建设提升到双向互动环境，提供在收看电视的同时实现在线购物的双向服务。

据美国电信工会的报告显示，从宽带网络接入方式看，韩国超宽带用户超过 1600 万个。而目前，韩国家庭宽带的普及率已经达到 95%，平均速率为 20.4Mbps，居全球宽带性能综合排名首位。但是，韩国政府仍不满足，其相关部门表示，韩国将建成在 10s 内即可下载完一部 DVD 级电影的千兆位宽带网。

## 1.3 中国宽带发展现状

近年来，我国宽带发展取得了长足进步，在国民经济和社会发展中发挥了重要作用。

### 1. 宽带在国民经济和社会发展中的作用逐步增强

① 宽带是推动经济增长的新兴力量。

2011 年，固定宽带和 3G 网络相关直接投资超过 2200 亿元，相关信息服务消费近 5000 亿元，并带动上下游关联产业实现产值超过 2.4 万亿元。

② 宽带是促进传统产业转型升级和培育新兴产业的重要基础。电子商务交易额接近 6 万亿元，软件外包、信息服务、云计算、物联网等新兴业态蓬勃发展，有力推动经济结构优化升级。

③ 宽带是拓展社会就业的重要渠道。2011 年固定宽带和 3G 发展带动通信设备、建设和服务开发等环节提供就业岗位超过 170 万个，带动电子商务、物流等关联产业提供就业岗位估计近千万个。

④ 宽带是促进公共服务和社会管理水平提升的重要支撑。基于宽带网络的教育培训、医疗卫生、电子政务、社会保障等得到广泛应用。

### 2. 宽带网络产业链明显提升

我国已形成覆盖光通信、宽带无线通信、下一代互联网、移动互联网、有线广播电视等多个领域的产业支撑能力，涵盖系统、终端、芯片、关键器件、仪器仪表等多个环节。已掌握光纤宽带接入、大容量长距离传输、高端路由交换、3G 移动通信等主流技术。宽带技术产品集成创新能力显著提升，部分国产宽带设备达到国际先进水平。在 TD-LTE、IPv6 等新领域取得核心技术突破。国际标准话语权不断增强。

### 3. 宽带网络覆盖和普及程度不断提高

① 网络能力大幅提升。宽带已覆盖全国所有城市、乡镇和 84%的行政村，超过 90%的宽带用户接入速率在 2Mbps 以上，有线电视双向化程度近 40%。国际出口带宽 2011 年达到 1.4Tbps，是“十一五”初期的 10 倍。

② 普及水平明显提高。2012 年 4 月固定宽带用户达到 1.59 亿户，比“十一五”初期增长 3.2 倍，宽带家庭普及率上升到 36.7%；3G 用户达到 1.59 亿户，在移动用户中占比提高到 15.4%。

③ 应用规模不断扩大。2012 年 4 月网民规模为 5.32 亿人，比“十一五”初期扩大了 4.8 倍，普及率上升到 39.7%；网页数量 866 亿个，增长了近 30 倍。

### 4．网络与信息安全保障能力持续加强

① 网络信息安全管理机制逐步健全。

② 网络信息安全技术手段、安全备份和应急处置能力不断增强。

③ 基础网络和重要信息系统安全等级保护、安全评测、风险评估等基础工作持续强化。

④ 网络关键装备可控水平和网络信息安全产业链能力明显提升。

**5. 我国宽带发展仍存在较大不足，面临着缓进则退的风险**

① 宽带网络差距有所拉大，我国宽带人口普及率与发达国家差距从 2005 年的 10%扩大到 12.8%，接入速度也不及全球平均水平。目前我国宽带普及仅为发达国家（25.6%）的一半；主流上网速率不到发达国家的四分之一。国际电信联盟数据显示，我国 ICT 发展指数（IDI，ICT Development Index）中的接入指标排名由 2007 年的第 64 位倒退到 82 位（倒退 18 位），而印度 IDI 接入指数由 129 位上升到 116 位（提升 13 位），巴西从 69 位上升到 66 位（提升 3 位），我国宽带发展与全球的绝对差距正在不断拉大。

② 农村和边远地区，因自然条件恶劣、人口居住分散、经济水平低下、网络部署成本过高，仅靠市场机制难以承担和持续运维，数字鸿沟继续扩大。到 2012 年年底，中西部宽带普及率落后东部 6%，农村宽带普及率仅为 5%，落后城市 12%。

③ 宽带网络性能与社会期望仍有较大差距，亟待同步提升网站接入带宽、内容分发网络布局和能力、用户宽带接入速率等，切实改善用户上网体验。

④ 宽带应用服务不够丰富，尚难以满足两化深度融合、中小企业发展、特色农村发展、促进社会公共服务信息化的迫切需求。

⑤ 宽带发展对下一代宽带技术产业提出更高速率、超大容量、绿色节能等新需求；宽带光通信产业链上游的高端光器件、关键芯片等环节对外依存度较大，进一步发展受到较大制约，急需突破关键技术，提升自主创新和产业支撑能力。

⑥ 城镇地区老旧小区宽带网络升级改造难，管道路权、基站选址、网络入户等无法得到政策保障，急需地方给予配套政策支持。

其深层次原因如下所述：

- 与国际相比，我国对宽带发展的紧迫性认识不统一，宽带基础设施地位仍不明确，全社会资源投入不足；
- 宽带发展缺乏顶层设计和统筹规划；
- 宽带市场竞争环境尚需完善，体制机制有待创新。

## 1.4 中国宽带发展目标

按照 2013 年 8 月国务院印发的《“宽带中国”战略及实施方案》（国发〔2013〕31 号），我国宽带发展的目标如下。

到 2015 年，初步建成适应经济社会发展需要的下一代国家信息基础设施。基本实现城市光纤到楼入户、农村宽带进乡入村，固定宽带家庭普及率达到 50%，第三代移动通信及其长期演进技术（3G/LTE）用户普及率达到 32.5%，行政村通宽带（有线或无线接入方式，下同）比例达到 95%，学校、图书馆、医院等公益机构基本实现宽带接入。城市和农村家庭宽带接入能力基本达到 20 兆比特每秒（Mbps）和 4Mbps，部分发达城市达到 100Mbps。宽带应用水平大幅提升，移动互联网广泛渗透。网络与信息安全保障能力明显增强。

到 2020 年，我国宽带网络基础设施发展水平与发达国家之间的差距大幅缩小，国民充分享受宽带带来的经济增长、服务便利和发展机遇。宽带网络全面覆盖城乡，固定宽带家庭普及率达到 70%，3G/LTE 用户普及率达到 85%，行政村通宽带比例超过 98%。城市和农村家庭宽带接入能力分别达到 50Mbps 和 12Mbps，发达城市部分家庭用户可达 1 吉比特每秒（Gbps）。宽带应用深度融入生产生活，移动互联网全面普及。技术创新和产业竞争力达到国际先进水平，形成较为健全的网络与信息安全保障体系。

我国宽带发展的技术路线和发展时间表如下。

遵循宽带技术演进规律，充分利用现有网络基础，围绕经济社会发展总体要求和宽带发展目标，加强和完善总体布局，系统解决宽带网络接入速度、覆盖范围、应用普及等关键问题，强化产业发展和安全保障，不断提高宽带发展整体水平，全面提升支撑经济社会可持续发展的能力。

### 1. 技术路线

统筹接入网、城域网和骨干网建设，综合利用有线技术和无线技术，结合基于互联网协议第 6 版（IPv6）的下一代互联网规模商用部署要求，分阶段系统推进宽带网络发展。

按照高速接入、广泛覆盖、多种手段、因地制宜的思路，推进接入网建设。城市地区利用光纤到户、光纤到楼等技术方式进行接入网建设和改造，并结合 3G/LTE 与无线局域网技术，实现宽带网络无缝覆盖。农村地区因地制宜，灵活采取有线、无线等技术方式进行接入网建设。

按照高速传送、综合承载、智能感知、安全可控的思路，推进城域网建设。逐步推动高速传输、分组化传送和大容量路由交换技术在城域网应用，扩大城域网带宽，提高流量承载能力；推进网络智能化改造，提升城域网的多业务承载、感知和安全管控水平。

按照优化架构、提升容量、智能调度、高效可靠的思路，推进骨干网建设。优化骨干网络架构，完善国际网络布局，全面推广超高速波分复用系统和集群路由器技术，提升骨干网络容量和智能调度能力，保障网络高速高效和安全可靠运行。

### 2. 发展时间表

（1）全面提速阶段（至 2013 年年底）

重点加强光纤网络和 3G 网络建设，提高宽带网络接入速率，改善和提升用户上网体验。

城市地区着力推进光纤化成片改造，农村地区灵活采用有线和无线方式加快行政村宽带接入网建设，提高接入速度和网络使用性价比。进一步提升城市 3G 网络质量，扩大农村 3G 网络覆盖范围，做好时分双工模式移动通信长期演进技术（TD-LTE）扩大规模试验工作。加快下一代广播电视网建设，推进“光进铜退”和网络双向化改造，促进互联互通。同步推进城域网扩容升级。以网间互连为重点优化互联网骨干网。推动网站升级改造，提高网站接入速率。

到 2013 年年底，固定宽带用户超过 2.1 亿户，城市和农村家庭固定宽带普及率分别达到 55%和 20%。3G/LTE 用户超过 3.3 亿户，用户普及率达到 25%。行政村通宽带比例达到 90%。城市地区宽带用户中 20Mbps 宽带接入能力覆盖比例达到 80%，农村地区宽带用户中 4Mbps 宽带接入能力覆盖比例达到 85%。城乡无线宽带网络覆盖水平明显提升，无线局域网基本实现城市重要公共区域热点覆盖。全国有线电视网络互联互通平台覆盖有线电视网络用户比例达 60%。

（2）推广普及阶段（2014—2015 年）

在继续推进宽带网络提速的同时，重点加快扩大宽带网络覆盖范围和规模，深化应用普及。

城市地区加快扩大光纤到户网络覆盖范围和规模，农村地区积极采用无线技术加快宽带网络向行政村延伸，有条件的农村地区推进光纤到村。持续扩大 3G 覆盖范围和深度，推动 TD-LTE 规模商用。继续推进下一代广播电视网建设，进一步扩大下一代广播电视网覆盖范围，加速互联互通。全面优化国家骨干网络。加强光通信、宽带无线通信、下一代互联网、下一代广播电视网、云计算等重点领域新技术的研发，在部分重点领域取得原始创新成果。

到 2015 年，固定宽带用户超过 2.7 亿户，城市和农村家庭固定宽带普及率分别达到 65%和 30%。3G/LTE 用户超过 4.5 亿户，用户普及率达到 32.5%。行政村通宽带比例达到 95%。城市家庭宽带接入能力基本达到 20Mbps，部分发达城市达到 100Mbps，农村家庭宽带接入能力达到 4Mbps。3G 网络基本覆盖城乡，LTE 实现规模商用，无线局域网全面实现公共区域热点覆盖，服务质量全面提升。互联网网民规模达到 8.5 亿人，应用能力和服务水平显著提高。全国有线电视网络互联互通平台覆盖有线电视网络用户比例达到 80%。互联网骨干网间互通质量、互联网服务提供商接入带宽和质量满足业务发展需求。在宽带无线通信、云计算等重点领域掌握

一批拥有自主知识产权的核心关键技术。宽带技术标准体系逐步完善，国际标准话语权明显提高。

（3）优化升级阶段（2016—2020 年）

重点推进宽带网络优化和技术演进升级，宽带网络服务质量、应用水平和宽带产业支撑能力达到世界先进水平。

到 2020 年，基本建成覆盖城乡、服务便捷、高速畅通、技术先进的宽带网络基础设施。固定宽带用户达到 4 亿户，家庭普及率达到 70%，光纤网络覆盖城市家庭。3G/LTE 用户超过 12 亿户，用户普及率达到 85%。行政村通宽带比例超过 98%，并采用多种技术方式向有条件的自然村延伸。城市和农村家庭宽带接入能力分别达到 50Mbps 和 12Mbps，50%的城市家庭用户达到 100Mbps，发达城市部分家庭用户可达 1Gbps，LTE 基本覆盖城乡。互联网网民规模达到 11 亿，宽带应用服务水平和应用能力大幅提升。全国有线电视网络互联互通平台覆盖有线电视网络用户比例超过 95%。全面突破制约宽带产业发展的高端基础产业瓶颈，宽带技术研发达到国际先进水平，建成结构完善、具有国际竞争力的宽带产业链，形成一批世界领先的创新型企业。

## 1.5　发展下一代互联网是“宽带中国”战略的重要任务

在《“宽带中国”战略及实施方案》（国发〔2013〕31 号）的技术路线中，明确提出我国宽带发展要统筹接入网、城域网和骨干网建设，综合利用有线技术和无线技术，结合基于互联网协议第 6 版（IPv6）的下一代互联网规模商用部署要求，分阶段系统推进宽带网络发展。在“宽带中国”战略的推广普及阶段（2014—2015 年），下一代互联网等领域的技术创新和规模部署成为重要的战略任务。明确提出了全面优化国家骨干网络，加强光通信、宽带无线通信、下一代互联网、下一代广播电视网、云计算等重点领域的新技术研发，在部分重点领域取得原始创新成果。

加速下一代互联网发展对于“宽带中国”战略实施具有重要意义。

在全球信息通信技术发生重大变革的关键时期，面对国际金融危机发生以来我国发展的外部环境和内部条件产生的巨大变化，我国加快发展下一代互联网具有重要的战略意义。

### 1．发展下一代互联网是抢占国际经济科技制高点的重要机遇

互联网发展水平已成为衡量一个国家综合实力的重要标志。为应对全球经济社会发展格局产生的深刻变化，世界各国尤其是主要大国在制定自身经济发展的战略

筹划中，都把发展互联网列为新一轮产业发展的重点。美国制定 IPv6 过渡计划的目的就是保持美国在互联网技术与市场上的主导地位，欧盟和日、韩也是想通过发展下一代互联网来抢占未来信息社会发展的先机和优势地位。同时美国等国家也高度重视其他国家和地区、特别是我国提早部署 IPv6 将会获取的利益，认为我国发展下一代互联网是为了占据互联网空间的重要份额，对其在互联网领域的霸主地位形成了挑战。因此从国际大环境来讲，下一代互联网已经成为国际经济科技竞争的战略制高点。

我国下一代互联网发展存在紧迫的需求。我国互联网用户规模全球第一，但是普及率仅为 31.8%，与发达国家 70%以上的普及率（美国 74.1%、韩国 77.3%、日本 74.1%）有相当大的差距。在提高网络普及率方面，我国具有很大的互联网发展空间。面对全球 IPv4 地址即将分配殆尽的严峻形势，我国 IPv4 地址短缺现象更为严重，现有的 IPv4 地址将于未来 1～2 年内分配完毕，发展 IPv6 网络已经迫在眉睫。解决地址短缺的现实问题迫使我国走到全球下一代互联网发展的前沿，使我国有望在全球率先实现下一代互联网大规模商用，为我国抢占国际经济科技竞争的战略制高点提供了难得的历史发展机遇。

实际上，基于 IPv6 与 IPv4 网络的建设成本基本相同的事实，我国越早发展以 IPv6 为基本特征的下一代互联网，越有利于国家基础设施的建设与发展，有利于降低技术换代的成本，有利于提升国家竞争力。

### 2．发展下一代互联网是培育战略性新兴产业的重要先导

加快培育和发展战略性新兴产业，是党中央、国务院顺应全球经济一体化、新技术革命方兴未艾的形势，为抢占新一轮发展的制高点作出的重大战略部署，是提升国家长远竞争力的关键举措。

信息产业是战略性新兴产业的重要领域之一。我国走信息化与工业化融合的新型工业化道路，要解决信息产业自身大而不强的问题，迫切需要寻找突破口，寻找新的增长点，以实现跨越式发展。而发展以 IPv6 为核心的下一代互联网为此提供了契机。因此，下一代互联网是发展战略性新兴产业的重要先导，能够引发社会新需求、引领信息产业结构调整和发展方式转变，带动并培育其他新兴产业，推动产业技术创新，抢占未来发展先机。同时，发展下一代互联网也为其他战略性产业的发展提供了支撑平台。

通过发展下一代互联网，可以进一步促进包括传感器网络在内的物联网、移动互联网等新兴产业的发展，带动传感器、RFID 芯片等核心技术的竞争力，缩小与发达国家的差距。发展下一代互联网将推动国家信息基础设施建设，带动社会信息化投资，给互联网设备制造业、软件业和信息服务业带来巨大的发展空间，带动信息产业发展。预计到“十二五”末，下一代互联网服务产业、软件和设备制造业的市场规模将超万亿元，并将带动其他产业的快速发展。

下一代互联网有利于推动三网融合，广电网络没有兼容现有 IPv4 网络的负担，可以直接采用 IPv6。通过广电网的双向改造，用户可以实现从看电视到用电视的转变，全国 4.2 亿台电视机将极大地丰富我国下一代互联网终端和应用，使我国信息技术和产业跃上一个新的台阶。

### 3．发展下一代互联网是转方式、调结构的重要推力

党的十七大强调，实现未来经济发展目标，关键要在加快转变经济发展方式等方面取得重大进展，促进经济增长由主要依靠增加物质消耗向主要依靠科技进步等方面转变。互联网技术是信息社会中的核心、关键和共性的战略高新技术。尽快开展下一代互联网的规模商用有利于使中国获得原始创新机会，有利于尽快占领下一代互联网核心技术的制高点，将会大大提高我国自主创新能力，加快经济发展模式转型，并通过用高新技术改造传统产业进一步促进产业结构调整。发展下一代互联网可加快网络基础设施建设、促进设备研发和产业化，推广新型业务应用，可显著带动社会投资和消费需求，为现代服务业带来新的发展机会，也为通信产业等结构调整打下基础，使我国走上创新驱动、内生增长的经济良性发展轨道。

### 4．发展下一代互联网是实现可持续发展、节能减排的重要途径

随着全球半数以上人口逐步进入现代化行列，能源需求和生态环境压力大幅提升，经济社会快速发展与地球有限承载能力的矛盾日益尖锐。作为工业化、城镇化快速发展的人口大国，我国面临的能源和生态环境矛盾尤为突出，推动可持续发展的任务尤为艰巨。全球发展面临的严峻挑战迫切需要创新经济发展方式，世界各国都在积极追求绿色、智能、可持续的发展。

发展下一代互联网，特别是推动物联网、移动互联网等需要大量 IP 地址的新型网络应用，有助于实现建筑节能、绿色照明、智能电网、智能交通、环境监测等，为我国实现可持续发展、节能减排提供了重要途径，对建设资源节约型、环境友好型社会，应对全球气候变化，维护中华民族的长远利益将会产生深远影响。

### 5．发展下一代互联网是缩小数字鸿沟、促进和谐发展的重要基础

由于我国城乡区域发展不平衡，在城市与农村之间、东部与西部之间存在着巨大的“数字鸿沟”，成为影响社会和谐发展的重要因素。发展下一代互联网，显著提高互联网的普及率，必将大大缩小城乡居民的数字鸿沟，为促进社会和谐发展提供重要基础。有助于实现教育的公平性，有助于人人享有基本医疗卫生服务，有助于提高社会的公共服务水平和应急响应能力，有助于构建社会化、网络化的服务体系，提高全社会创新效率，促进知识成果传播、转化、应用。有助于全面促进社会进步和提高人们生活质量。

### 6．发展下一代互联网是应对网络霸权、维护国家安全的重要契机

当前，国家安全已经从海、陆、空等维度扩展到网络空间，网络安全已经上升为主要的安全挑战。国际上，以美国为首的发达国家高度重视互联网发展，将其作为维护国家霸权的重要手段，建立网络安全攻防体系。在国内，作为国民经济和社会发展的重要基础设施，互联网自身的安全及以互联网为重要基础的国家安全也面临着严峻的挑战。因此，把网络安全作为国家安全的重要组成部分，建立强大的网络与信息安全保障体系，对我国的经济增长、社会的稳定与发展具有重要的战略意义。

下一代互联网为解决安全问题提供了新的技术平台，提供了从总体上构建更加安全可信的下一代互联网的发展机会，有利于逐渐改变我国互联网受制于人的不利局面，实现网络安全自主可控。

# 第 2 章 下一代互联网发展及演进目标与路径

**本章要点**

- ✓ 互联网面临的需求与挑战
- ✓ 下一代互联网的发展目标

## 本章导读

经过四十余年的发展，互联网已成为人类社会的重要基础设施和国家的重要战略资源。作为网络空间（Cyberspace）的基石，互联网正处于技术变革和向下一代升级演进的关键时期，以满足信息社会对网络空间基础设施安全可信、可管可控、泛在可靠的基本要求。美欧等纷纷加快战略布局，加强未来网络技术研究与试验，抢占网络空间基础设施的主导权，战略意图和战略布局日渐清晰。我国应抓住网络技术变革带来的技术格局、产业格局和网络空间主导权调整的难得机遇，从战略高度重视网络空间基础设施的发展，尽快明确战略定位和重点，加快未来网络技术创新和试验，提升我国网络技术与产业能力，争取网络空间基础设施的主动权，塑造未来信息社会中网络空间基础设施的国家竞争新优势。

互联网处于技术变革与升级演进的关键时期。现有互联网存在着业界公认的地址空间不足、服务质量难以保证、安全可信机制缺乏、网络管控能力差等突出问题，自 20 世纪 90 年代以来，学术界和产业界为之付出了不懈的努力，但是这些问题是由互联网采用的 TCP/IP 协议族所决定的，因此至今不但没有彻底解决，而且随着互联网的快速普及和深入应用，问题还变得越来越突出。未来信息社会对网络空间基础设施提出了安全可信、可管可控、泛在可靠的基本要求，面对这些要求，现有互联网面临着技术变革，处于向下一代升级演进的关键时期。

目前，互联网近期演进路径比较清晰，国内外认识也较为统一，但是中远期发展路径尚未明确，技术发展方向正在探索之中。

从近期来看，由于 IPv4 地址已基本耗尽，移动互联网、物联网的发展面临着地址不足的瓶颈性制约，IPv6 能够提供海量地址空间，是目前唯一成熟可用的下一代互联网解决方案，因此目前业界普遍认为 IPv6 是下一代互联网演进的起点。近几年国际上 IPv6 发展呈加速态势，我国也明确了 IPv6 商用部署的路线图和时间表，开展了 IPv6 网络规模建设，按照国家规划，未来 5 年将实现 IPv6 的规模应用。

对于互联网中长期发展路径，考虑到 IPv6 规模商用以后，在未来几年将形成庞大的网络规模和用户规模，抛开这些基础从头新建一个网络并不现实，因此一般认为互联网中长期是基于 IPv6 网络演进的或是兼容 IPv6 网络的。由于 IPv6 只解决了互联网地址空间不足的问题，不能解决现有互联网的其他问题，因此 IPv6 不是下一代互联网的全部，需要基于 IPv6 网络持续开展网络技术创新。

美欧等十分重视网络技术创新，纷纷加大研究支持力度，积极开展未来互联网（Future Internet）的研究与试验工作。在国内通常将未来互联网称为未来网络、下一代互联网。尽管未来互联网、未来网络和下一代互联网的称谓不同，但是它们的发

展目标和基本内涵是一样的，都是互联网中长期演进的愿景、网络空间基础设施的核心组成部分。

# 2.1　互联网面临的需求与挑战

## 2.1.1　互联网的可持续发展面临严峻挑战

互联网最初是为单一的数据通信需求而设计的，其设计目标是实现网络的健壮性和支持底层网络技术的异构性，并且默认互连的用户属于相互信任的团体。因此，传统的互联网体系结构仅支持尽力而为的服务，遵循“核心简单，边缘智能”的设计原则，网络智能地部署在网络边缘的终端上。这种体系结构简单，但保证了高效的互通和良好的演进性，并且一直沿用至今。

互联网及其应用的发展如图 2-1 所示。


图 2-1　互联网及其应用的发展

随着 20 世纪 90 年代互联网步入商业化时代，互联网的性质已经从一个以科研为主要目的的网络演变为全球规模的信息基础设施。近年来，随着网络技术的高速发展，出现了大量新型接入技术，如 WiMAX、WiFi、无线局域网、蓝牙，以及大量新型异构网络（如移动自组织网络、无线传感器网络、网状网）、大量新的计算技术（如 P2P、网格、普适计算和多样化的应用），这些新技术和应用在推动整个通信

领域进步的同时，也使得传统互联网体系结构面临着巨大的挑战。复杂的异构网络环境增加了维护管理的复杂度，同时也影响了网络的灵活性、健壮性和安全性；无处不在的应用需求要求互联网支持移动性；多样化的应用要求互联网支持不同实时性的业务。随着网络复杂度的增长，传统的“核心简单”的互联网难以满足网络对可控、可管的迫切需求，已经运行了 40 年的以 IP 协议及相应编址路由机制为核心的互联网基础架构越来越不堪重负，互联网的可持续发展性面临着严重的挑战。

现有网络体系结构在面对目前的应用需求时，都存在着一些问题，对这些问题的反思对于未来网络体系结构的研究有着重要意义，是研究的出发点。

### 1. 在安全性方面

通常认为传统电信网络是安全的，因为电信的网络层次和网络区域是严格定义的，用户只能看到 UNI 接口，而 NNI 和 SNI 以上的网络和应用用户是不能直接访问的。而在互联网中，由于网络的端到端透明性和网络的扁平化，用户可以访问网络中的任意网元，可以对网络中的设备进行攻击，网络安全性较差。当前互联网的安全隐患存在于设计、实现、运行管理的各个环节，频繁暴发的互联网安全事件是安全问题的具体表现，互联网络的安全事件增长趋势已远远超过了互联网规模的增长速度，安全问题已经成为困扰互联网发展的首要难题。

（1）现有的互联网在设计阶段没有充分考虑安全问题，缺乏一个系统的安全体系结构，在 TCP/IP 底层协议没有完善的内置安全机制，现有的安全技术都是以修修补补的形式增加进来的，因此难免会出现安全漏洞、功能重叠、实现复杂等各种问题。

（2）在网络操作系统及网络协议实现中存在大量安全漏洞，给安全入侵者带来了可乘之机。

（3）在现有网络运行和管理阶段，计算机软件和硬件系统在实现过程中的脆弱性导致各种安全漏洞或安全机制与管理政策之间的不一致性是普遍存在的。因此可以看出互联网在安全性方面的缺陷是体系结构上的缺陷，是需要对体系结构进行调整才能够根本解决的。

因此在未来网络的体系结构研究中，网络安全性是否能够从体制上进行保证是检验网络体系结构是否合理的重要依据。

### 2. 在移动性方面

对于互联网来说，泛在要求网络能给用户提供无时不在、无处不在、无所不有的综合服务，面向固定位置主机和单一数据服务而设计的传统互联网远远达不到泛在的要求。

（1）互联网尚未很好地解决移动问题。由于最初的 TCP/IP 协议体系是面向固定

位置的主机而设计的，IP 地址被赋予双重功能：一是表示主机所处的位置，用于网络层路由；二是标识主机本身，用于建立传输层的连接。这种功能耦合导致无法支持主机和 IP 地址的动态绑定，进而无法很好地解决主机的移动问题。

（2）大量智能移动设备如笔记本电脑、掌上电脑甚至手机等移动通信工具都有享用互联网服务的需求，以及未来的很多智能设备都可能连网，但是目前互联网还不能支持如此丰富多样的接入技术。

（3）目前的互联网服务多为集中的客户-服务器模式，还不能达到广泛综合和无处不在。传统电信网络的体系结构形成时，移动通信需求还不是十分强烈，因此其体系结构中未考虑终端的移动性。移动性是后来才补充到电信网络中的。因此在采用自顶向下方法研究未来网络的体系结构时，需要对移动性和泛在性进行充分考虑，以在体系结构方面更好地支持移动和泛在需求。

### 3. 在网络性能方面

在目前的互联网协议体系结构中，网络性能和服务质量保证是一个难题。互联网本质上提供的是一种“尽力而为”的无连接的服务，它的功能只是尽量将分组发送到目的端，但是不提供任何服务质量保证，如吞吐率、延迟和抖动。在以 FTP、E-mail、Web 服务为主的数据业务环境下，互联网基本能够满足用户需求，但是对网络服务质量要求较高的大量新的应用如语音电话、IPTV 等实时流媒体传输，互联网难以提供足够的性能和服务质量。由于传统电信网络是有信令存在的，是面向连接的，两端在通信之前已经建立好了通道（虚电路），并且已经进行了资源预留，因此只要通过接纳控制的通信要求，均能在后续通信中对其服务质量进行保证。对网络性能和服务质量的保证也需要在网络体系结构上进行考虑，从而从本质上解决这些问题。

### 4. 在可管可控性方面

网络可管理性方面的欠缺也是互联网体系结构方面的问题。互联网的核心理念之一是对于数据进行无记忆传送，在网络中尽量不保存或少保存状态信息，从而保证网络设备的简单和高效。这种理念使得网元中缺少用于管理的必要信息，使得管理员无法高效地对网络进行管理和控制。目前的互联网管理还依赖于最初的管理技术手段（基于网元级别的管理系统进行管理），操作复杂、效率低下，难以适应现有的规模庞大结构复杂的网络系统。电信网络中是十分注重网络的可管理性的，在其体系结构中已经包含了对网络和业务状态信息的收集和管理，并且在行业内也已经制订并形成了系统的网络管理体系，因此一般认为电信网络的体系结构在网络管理性方面并不存在欠缺。对整个网络而非单个设备的管理、自动化的网络管理和配置工具、强大的分布式的网络监控、错误预警和快速发现、全局的用户行为跟踪控制

等问题亟待解决。

5. 在可信性方面

互联网在可信任机制方面存在欠缺，这种欠缺也是由互联网的体系结构所决定的。互联网的开放和匿名特征使得互联网的可信任性一直无法保证，大量的非法入侵、地址欺骗、身份假冒、网络欺诈等事件就是信任危机的具体表现，而且绝大多数事件无法追踪到肇事者。

（1）互联网设计初期认为用户都是一些可信的科研人员，没有考虑任何信任机制。实际上目前的互联网用户成分复杂，不乏大量恶意的用户进行破坏，这是安全问题盛行的直接原因。因此，急需引入对上网用户身份的认证机制，确保可信的网络环境。

（2）现有互联网中的路由设备基于目的地址转发分组，使网络中间节点对传输数据包的来源不做验证、不做审计，导致地址假冒、垃圾信息泛滥，大量的入侵和攻击行为无法跟踪。

（3）目前大量的网络用户使用私有地址，通过地址转换（NAT）方式接入互联网，导致安全事件的追踪极为困难。

（4）尚缺乏能够广泛使用的端到端的身份认证机制。由于现有互联网的不可信任性，许多关键的业务系统构建在现有不可信任的互联网上，存在着极大的风险，阻碍了信息化的发展进程。

电信网中由于有严格的区域划分，存在 UNI、NNI、SNI 接口，同一运营商 NNI 以上部分均认为是可信任的，不同运营商之间的网络通常也认为是可信任的，因此一般认为，传统电信网络的网络体系结构在可信任机制方面是不存在缺陷的。网络的可信任机制是网络体系结构中应该重点考虑的问题之一，也是检验体系结构合理性和可行性的重要依据。

## 2.1.2 全球对下一代互联网的研究风起云涌

面对当前互联网所面临的问题，同时也为了抢占未来信息技术的制高点，美、欧、中、日、韩等国家和地区都纷纷开展了对未来互联网的研究。这些未来网络研究计划的研究目标大多着眼于 10～15 年之后可以取代现有 Internet 的新型网络。其中具有代表性的项目有：

- 欧盟 FP7（第七框架计划）中未来互联网相关的 4WARD、FIRE 项目等；
- 美国 NSF 支持的 FIND、GENI、PlanetLab 项目等；
- 中国的 FPBN、层次化网络、普适网络等；
- 日本的 AKARI、JGN2+等。

其中，美国和欧盟是目前全球未来互联网研究的中心。

1. 美国

美国凭借其在互联网领域的先发优势，一方面希望通过维护现有互联网治理格局、坚持现有互联网技术体系来继续巩固和强化其在互联网领域的霸权地位；另一方面，美国也充分认识到现有互联网存在的突出问题，加紧未来网络的超前布局，强化未来网络技术创新与试验，希望将现有优势延续到互联网长期演进中。

美国国家科学基金会（NSF）负责未来网络的研究与试验工作。从 2002 年开始，NSF 相继启动了 GENI 计划（全球网络创新环境）和 FIND 行动（未来互联网网络设计），其中 GENI 计划侧重于分阶段建立支撑网络架构和关键技术研究的试验验证平台，目前已经建立了覆盖全球的具有 2000 多个节点的试验网络。FIND 行动资助了近 50 个未来网络相关的研究项目，侧重于互联网网络架构及关键技术的研究与创新，致力于基础研究，解决未来网络系统架构的一系列基础性问题，更加关注细节和协议。

2010 年 NSF 重点赞助了 5 个未来网络研究项目：ChoiceNet、NEBULA、MobilityFirst、XIA、NDN，逐步将未来网络的研究项目重点聚焦于多业务支持、云计算、移动性、网络基础架构（基于名字的路由）等。这些研究项目对全球未来网络技术发展方向具有重要影响，研究水平处于全球领先地位，成为其他国家跟踪研究的重点，也代表了未来网络技术研究的重要方向。

（1）ChoiceNet 项目

ChoiceNet 强调网络的开放性，试图通过全新架构的设计将协议栈各层的功能向用户开放，建立一个包括用户、服务提供商及开发商在内的生态系统，让用户任意选择技术和服务，实现网络经济性的最大优化。

（2）NEBULA 项目

NEBULA 面向云计算数据中心互连需求，构建全新的网络架构，将未来网络带入一个“云”化的模式，实现互联网的在线快速资源供应、公用定价和在线管理。

（3）MobilityFirst 项目

该项目旨在解决网络移动性问题，通过研究建立“全面延迟容忍网络”（GDTN）来提高通信稳定性，关注移动性和扩展性的平衡，充分利用网络资源来实现移动端点间的有效通信。

（4）XIA 项目

XIA 旨在解决网络使用多样性和可信传播问题，实现网络可重构，确保了传播

路径的灵活多样和安全。

（5）NDN 项目

NDN 旨在解决内容的高效分发问题，通过重新设计命名、编址、路由来实现全新的网络架构，使互联网可以不考虑内容存储所在的物理位置而直接面向内容进行数据分发。

美国未来互联网的研究主要由 NSF 和各大高校来推动。从 2005 年开始的 FIND（Future Internet Network Design）计划最初资助了近 50 个未来互联网相关的研究项目。在 2010 年，NSF 逐步将未来互联网的研究项目重点聚焦于多业务支持、云计算、移动性、网络基础架构（基于名字的路由）等四个方面。同时，美国还大力加强试验床的建设，PlanetLab 已经在全球部署了 520 个站点，拥有 1138 个节点，其战略意图就是成为未来互联网的骨干基础设施。

### 2．欧盟

欧盟期望抓住网络技术新一轮变革的机遇，摆脱在现有互联网发展格局中一直以来对美国的跟随态势，实现欧盟在互联网领域对美国的赶超。2007 年 1 月启动的欧盟第七框架计划（FP7）中，启动了“未来互联网研究和实验（FIRE）”项目，加强互联网体系结构及关键技术研究，以及未来网络实验床的建设，目标是建立欧洲未来互联网实验平台，支持有关解决网络可扩展性、复杂性、移动性、安全性及透明性问题的新方法研究。

欧盟在其 FP7 计划中资助了众多未来互联网方面的研究项目，主要可以分为业务、媒体、物联网、安全、网络架构、试验床等六方面的内容，其中最重要的部分是对未来互联网基础架构的研究和试验床的建设，仅 FIRE（Future Internet Research and Experimentation）试验床项目的投入就达到了 4000 万欧元。

在网络体系结构与关键技术研究方面，每年均启动近百个研究项目，重点支持内容路由、P2P 等网络传输层技术研究，CDN 和 IDC 等应用基础设施层的技术创新，以及云计算、移动互联网、物联网等典型应用的业务创新。这些项目的研究成果均要在 FIRE 支持的未来网络试验床上进行试验验证。

在未来网络试验床建设方面，一方面建设针对特定技术方案的专用试验床，如 WISEBED（Wireless Sensor Network Testbeds）为大规模无线传感器测试提供了多层基础设施；另一方面，通过联邦制整合既有试验床资源，构建通用的联邦试验床。例如 PII 项目，致力于研究如何通过联邦方式把现有的试验床及正在建设的试验床进行集成，实现这些专用床和通用床的长期持续发展。目前欧盟的 FIRE 试验床已经具有近千个节点，实现了与美国 GENI 试验床的互连。

### 3. 日本

日本十分重视未来网络的研究工作，启动了一批未来网络研究项目，其中最有代表性的是国家情报与通信技术研究所（NCIT）启动的 AKARI 项目。AKARI 项目旨在研究下一代网络架构和核心技术，解决现有 IP 化网络在安全性、移动性、资源管理方面存在的不足。整个项目的研究分为四个层面：应用层、覆盖层、IP 层和底层。该项目对未来网络有三个核心方面的定义：① 简洁与智慧网络；② 实体连接；③ 可持续与可演变。项目自 2006 年启动以来，取得的成果涉及平行光分组传输理论、全光路径/分组交换、包分多址、身份/位置分离和网络虚拟化等领域。该项目预期在 2016 年初步研究形成未来网络的基本架构。

### 4. 韩国

早在 2005 年，韩国就开始了互联网新型网络架构的研究工作，并在 2010 年成立了“放送通信委员会”，出台了《未来网络促进战略》，其目的是未来网络将融合通信、广播、计算机、传感网，组建一个能够随时随地不间断地提供符合用户特点和状态的最佳服务的环境，并且能够突破现有网络结构的局限，建立一个能够接受融合服务和多元终端的技术及服务模型。其方针是确保韩国在服务、终端、网络架构等所有领域的技术力量，通过解决社会现有问题及创造新市场，将未来网络作为可持续发展的绿色成长动力和韩国在 21 世纪经济发展的新动力。

美国和欧盟未来互联网研究的范畴如图 2-2 所示。


图 2-2　美国和欧盟未来互联网研究的范畴

综合美、欧等国家和地区对未来互联网的研究方式，其基本思路是从理论研究和实验平台两个方面同时推进：一方面，进行创新体系结构、交换与传输体制、关键算法等方面的理论探索；另一方面，建设可以对这些理论研究成果进行大规模、真实用户测试验证的实验网络平台。这种推进方式和策略值得我们学习和借鉴。

# 2.2 下一代互联网的发展目标

## 2.2.1 互联网面临的核心挑战和网络目标

### 1. 对未来互联网的要求

当前的互联网已经成为全球的信息基础设施，同时承担了商业化平台、社会信息载体、大众通信工具、新型公众媒体等多重职能，其产业链也日趋复杂，产业链上各个环节都对互联网提出了越来越高的要求。

- 用户：用户需要网络具有较强的安全能力，一方面保障终端、客户网络的安全；另一方面保障用户隐私信息的安全；同时用户不断增长的业务需求也对网络业务承载能力提出了更高的要求，如组播业务支持、移动性支持等。
- 网络运营商：互联网对于网络运营商来说不仅是一个传送信息的管道，而且应该是一个可管理、可运营，具有丰富灵活的网络资源，同时能够迅速拓展新业务的平台。
- 内容提供商：对于内容提供商来说，不仅要关注网络的质量，即用户的应用感知问题，而且要提高资源利用效率，降低运营成本。
- 政府：互联网是一个崭新的社会信息、舆论平台，对于政府来说一方面要关注互联网对社会生活的影响，面对互联网带来的网络犯罪、网络攻击等新的危害社会的问题；同时蓬勃发展的互联网也成为全球新的能耗大户，未来将成为节能减排工作的关注重点。

### 2. 未来互联网面临的挑战

目前互联网所表现出来的一系列问题可以归结为互联网所面临的六大挑战：

- 地址资源耗尽；
- 全球路由爆炸；
- 业务模式缺乏灵活性；
- 网络安全问题严重；
- 业务应用质量无法保证；
- 能耗压力日增。

### 3. 未来互联网的关键目标需求

未来互联网的目标就是解决目前互联网所面临的挑战，为全社会提供一个支持

多种业务应用、安全可靠、具有服务质量保证、网络资源丰富且可扩展、能够满足绿色节能要求的网络平台。据此可以总结出未来互联网的关键目标需求，包括：

- 地址资源充足；
- 网络层路由具有高度扩展性；
- 支持多种业务模式及网络结构；
- 安全可信、可管理可控制；
- 能够保证服务质量；
- 符合绿色节能需求。

只有能够很好地完全满足这些需求的网络体系结构才是可以接受的。

（1）安全性方面

未来的网络协议体系结构需要满足四个基本的安全要求：① 信息的保密性，确保信息不会被未授权的用户访问；② 数据完整性，确保信息在传输途中未遭到任何改变；③ 可认证性，用户能够确认通信对端的身份；④ 不可否认性，用户发出一条消息之后不能否认自己发出了这条消息。

完整性是指防止对信息的篡改，保密性是指防止信息向未授权的第三方泄露，可用性是指防止资源或信息的未授权持有和保留，鉴权是验明登录到系统的用户身份的过程，授权是允许被授权用户访问敏感信息、受保护业务或资源及执行受控操作的行为。为实现这些目标，下一代互联网需要建立安全性框架。在路由器、无线网络控制器、网关、服务器等网络组件中架构安全性平台（如入侵检测、病毒防火墙），保证设备的完整性和高可靠性，进行故障恢复。此外，还需在通信协议中增加安全性措施，以保护数据传输通道，并对数据加密以保护信息内容。

未来互联网的目标特征如图 2-3 所示。


图 2-3　未来互联网的目标特征

未来的网络必须提供攻击发生前的安全预防、攻击发生时的报警响应及攻击发生之后的审计追踪，达到三位一体的综合安全。从水平方面看，将涉及网络安全域

的划分、用户接入安全机制、安全域内部和安全域之间的安全机制；从网络功能组成方面看，将涉及用户平面与网络控制和管理平面的隔离机制。

（2）移动性方面

未来的互联网需要给用户提供无时不在、无处不在、无所不有的综合服务，支持通信终端的无缝快速移动，支持丰富多样的终端接入技术，支持大规模的分布式泛在服务，使网络就在用户身边。

（3）网络性能方面

未来的承载网络要支持高带宽的应用，提供更快、更流畅、更丰富的多媒体数据传输。能够以合理的价格提供用户所需的服务质量，并且能够为多种业务提供不同的网络环境，这些网络环境在网络性能方面是个性化的。即未来的承载网络需要支持多样化的服务，既要支持“尽力而为”的服务，又要根据需求来提供具有保证的服务，支持用户业务类型划分、优先等级处理和服务质量保障机制，以及网络资源的分配和使用管理机制，提供满足业务级合同（SLA）的用户服务，从而有利于运营商构建更合理的商业模式，也利于用户享用网络的方便性。

（4）可管可控性方面

未来的网络管理需要简单高效，适应规模庞大结构复杂的网络系统。不仅提供对单个设备的管理，而且提供对整个网络的管理和控制；不仅提供手动管理，而且提供自动化的网络管理和配置工具；支持大规模分布式的网络监控，支持错误预警和快速发现，支持全局的用户行为跟踪控制。提供方便、准确和开销低的网络运行管理和维护（OAM）机制，应能在不中断用户业务的条件下进行服务质量检测，提供迅速、准确的网络故障定位能力。

（5）可信性方面

第一，未来的网络需要提供用户身份认证机制，确保只有可信的用户才能访问网络或服务。第二，未来的网络需要对传输数据包的来源做验证和审计，防止地址欺骗等不可信行为。第三，未来的网络需要建立跨域的全局认证体系。第四，建立一个针对用户的信誉模型，为可信任的应用提供基础。第五，网络需要建立可信度的度量，向用户提供可信服务，并需要网络安全、控制和管理等各种机制协同达到可信度的指标。

（6）网络过渡方面

未来网络的网络体系结构要能与现有 IP 网络在一定层次上兼容，从而保证网络

的共存、互联互通、平滑过渡。

（7）支持多种业务方面

未来网络要承载多种业务，提供开放、完备和灵活的新业务支撑网络环境，应能支持扩展已有业务和接入第三方新业务，同时支持新业务的快速开发、推广。

（8）兼容底层异构网络方面

未来网络要成为通用的承载网络，就要向下兼容多种异构网络。IP 网络对底层异构网络的兼容性是其取得成功应用的基础。

### 4. 未来网络的演进目标

现有互联网是建立在 20 世纪 70～80 年代发明的 TCP/IP 协议基础之上的，随着互联网的全面普及与应用，其网络地址空间不足、安全可信机制缺乏、服务质量难以保证、内容分发机制不健全、网络监管困难等问题越来越突出，在很大程度上制约了互联网自身的发展。互联网作为全球的战略性信息基础设施，其下一步的技术演进尤为关键，当前正处于技术变革和向下一代升级演进的关键时期。

互联网的近期演进路径较为清晰，国内外认识也较为统一，即 IPv6 是下一代互联网演进的起点和基础。但是 IPv6 不能解决互联网的上述所有问题，不是下一代互联网的全部。互联网的中长期演进需要基于 IPv6 加强技术创新与应用，不断解决互联网发展问题，提升网络能力。

未来网络面向互联网中长期演进需求，致力于研究建立地址充足、安全可信、泛在可靠、分发高效、可管可控的互联网网络架构和网络基础设施。未来网络在欧、美、日、韩等国也被称为新一代互联网或未来互联网，但是这些名称总的来看并无实质性的区别，都是面向互联网的可扩展性、安全性、移动性、服务质量保证、内容分发等需求来探索互联网的中远期发展与演进路径的。即未来网络是对下一代互联网中长期演进目标网络体系的一种称谓。

### 5. 未来网络演进的路线

对于互联网中长期发展路径，目前国际上有渐进式路线与革命式路线之分。因此未来网络既可以是渐进式路线也可能是革命式路线。

渐进式路线采用与现网兼容的演进方式，即基于现有 TCP/IP 协议进行技术创新，不断完善现有互联网技术体系，逐步解决互联网现有问题，注重技术改进的实用性。其主要特点是基于 IPv6 数据传送格式和无连接分组交换节点转发方式，通过改变路由控制策略向未来网络演进。

革命式路线是指直接面向新需求，不考虑与现网兼容，重新设计网络基础架构，力图从根本上满足各种需求。革命式路线侧重于技术的超前研究，试图从根本上改变 TCP/IP 体制，寻求根本性的突破。日本的新一代互联网以提出网络新体系为目标，定位在今后 15 年的网络。美国的 FIND、FIA 都是以未来互联网命名的研究计划，其后的 GENI 计划明确立足革命式路线，但这些项目的研究难度很大，在一个小范围的试验网上的研究成果难以证明在大网上是否可行，项目的进展远未达到预期。

在互联网长期演进过程中，渐进式路线与革命式路线是相互借鉴、相互促进的。ITU-T SG13（未来互联网研究组）主导 ITU 的未来网络技术标准研究工作，目前已经完成并发布了 ITU-T Y.3001“未来网络：指标与设计目标”，其中对于“未来网络”给出了比较宽泛的定义，该定义并没有在未来网络研究中明确肯定或否定 TCP/IP 技术体系，包括了全新的和改进的网络体系的两种可能性，以及新型网络架构与现有网络融合发展的可能性。因此，任何一种针对当前互联网面临的重大技术挑战、面向未来 15～20 年应用需求的新型网络，无论是渐进式路线还是革命式路线，都属于未来网络的概念范畴。实际上，美国 NSF 支持的 5 个 FIA 未来网络项目并不都采用革命式路线，其中有的项目采用的是渐进式路线。

## 2.2.2 下一代互联网技术要素模型

从技术的发展历程来看，互联网整体结构的发展是一个从核心到外围、从基础架构到外部需求的过程。

最初互联网的技术核心就是 TCP/IP，以及与之密不可分的路由技术、资源与地址的映射技术等，这些基础技术可以归结为解决网络的命名、编址、路由问题，解决了这些基本问题，IP 网络就构成了一个可以实现端到端数据传送的通信网络。

随着网络的发展和应用的丰富，各种应用和网络拓扑结构对 IP 网络提出了更多要求，需要网络在满足基本通信需求的基础上，进一步扩展业务支持能力。

当网络发展到社会信息基础设施阶段，社会各领域又对网络提出了安全可靠、可运营管理、绿色节能等需求，这些需求实际上来自于网络技术发展的范畴之外，但必然会对网络技术的发展构成重大影响。

总结以上的分析，可以结合未来互联网的目标特征，归纳出互联网的技术要素模型。这个模型应该是以互联网的核心架构（命名、编址、路由及相应的资源管理模式）为基础，逐步扩展到业务支持能力（如终端移动性、组播或广播能力、用户多接入等），同时还需要对来自社会其他领域的外部需求（如安全、服务质量、绿色节能等）提供支持，如图 2-4 所示。

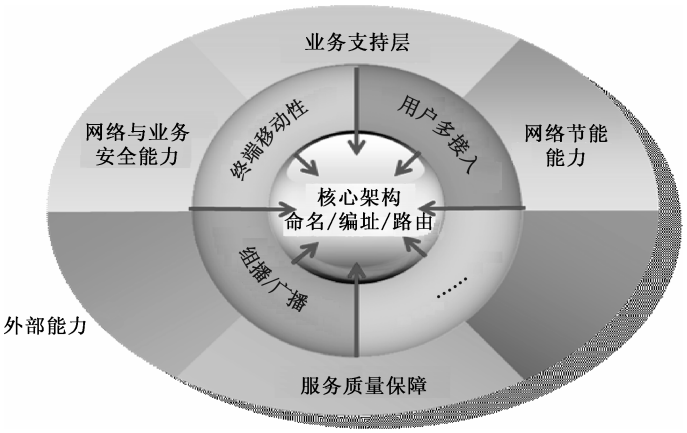



图 2-4　互联网技术要素模型

在这个要素模型中，互联网的核心架构是最关键、最基础的部分，其他各个层面的技术需求实际上最终都需要反映到核心架构所能提供的基础能力上，或者需要核心架构进行相应的改变或完善。

从目前互联网的发展趋势来看，出现了两种发展路线：一是所谓“改良路线”，即在现有互联网基础之上的演进，通过一些改良性的技术，在不改变互联网核心架构的基础上对网络能力进行完善；二是所谓“革命路线”，根据互联网的需求模型重新构建网络的基础架构，使新的网络能够从根本上支持各种外部需求。实际上这两种路线最根本的区别就是是否要对互联网的核心架构进行改变，我们认为这也是区分改良路线或革命路线最关键的标志。

## 2.2.3　下一代互联网的两种思路在融合中发展

对于向未来互联网演进的所谓“改良路线”和“革命路线”来说，虽然它们之间有很多根本性的区别，二者之间并不是完全排斥或互不兼容的。对于互联网未来的演进方式，目前没有人能够清晰地描述出来，而这两种路线也在融合中共同发展，如图 2-5 所示。

一方面，“革命路线”所描述的未来互联网的目标特征来自于当前互联网中的业务与用户需求，同时，当前的互联网也为“革命路线”的研究提供了网络和应用的参照；另一方面，“革命路线”的研究为现有网络的改良提供了众多可以参考的思路，如目前已经提出的解决路由扩展性问题的 LISP（Locator/ID Separation Protocol，身份/位置分离协议）、HIP（Host Identity Protocol，主机身份协议）等方案都借鉴了“革命路线”中关于地址与路由的层次化思路。

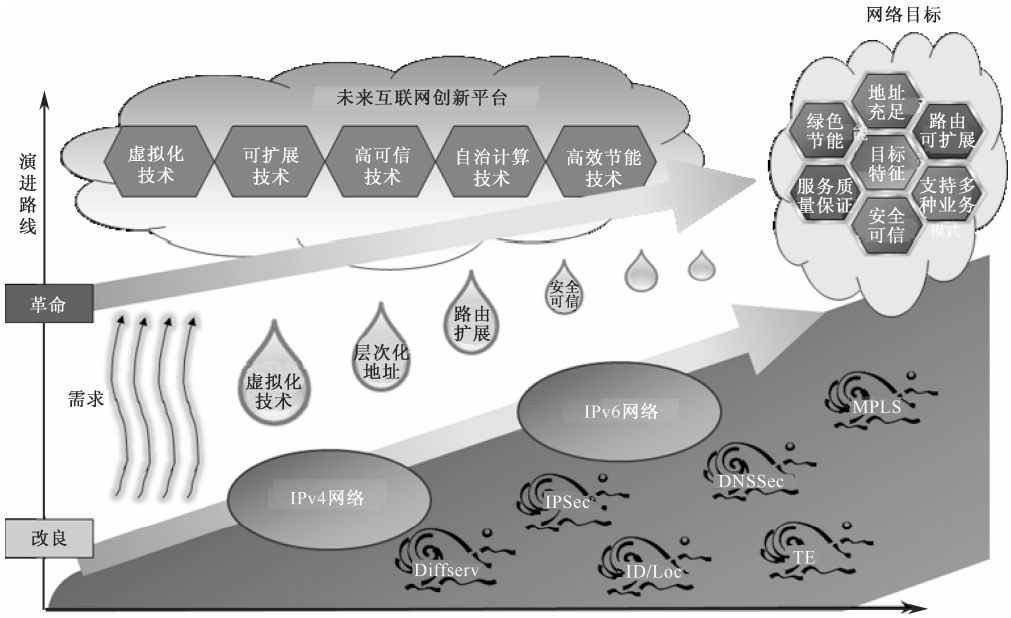



图 2-5　两种路线在融合中发展

# 第 3 章 IPv6 技术特点及过渡机制

**本章要点**

- ✓ IPv6 技术的特点
- ✓ IPv6 地址格式
- ✓ IPv6 包头格式
- ✓ IPv6 基础协议
- ✓ IPv6 路由机制
- ✓ IPv6 网络过渡技术


IPv6 以其丰富的地址资源解决了现有 IPv4 网络地址不足的问题，并为网络移动性、网络安全性的改善提供了一定的条件，经过 20 多年的发展与实践，已经成为目前唯一较为成熟的下一代互联网解决方案。尽管其并未彻底解决网络安全、网络扩展等核心问题，但是基于IPv6网络技术可以逐步融合新的网络技术理念和技术要素，可以长期持续升级演进，因此被业界认为是下一代互联网升级演进的起点。

## 3.1 IPv6 技术的特点

互联网协议第六版（IPv6）是互联网协议的一个新的版本，IPv6 是 IETF（互联网工程任务组，Internet Engineering Task Force）设计的用于替代现行版本 IP 协议（IPv4）的下一代 IP 协议，其基本协议在 IETF RFC 2460 中规定。IPv6 相对于 IPv4 的主要改变如下。

（1）扩展的寻址能力

IPv6 把 IP 地址空间从 32 比特增加到了 128 比特，从而能够支持更多层次的寻址结构、更多的可寻址节点的数量，以及更为简化的地址的自动配置。IPv6 通过在组播地址中加入一个“范围”域而提高了组播选路的扩展性。在 IPv6 中还定义了一种称为“任播地址”的新的地址类型，它被用来向一组节点中的任一个节点发送数据包。

（2）简化的头格式

IPv6 省略了一些 IPv4 头中的域或将其改成了可选项，从而减少了数据包的公共处理开销，并减少了 IPv6 头所占的带宽开销。

（3）对扩展和选项的增强支持

IPv6 在 IP 头选项的编码方式上作了一些变化，其目的是更有效地进行转发，并放宽了对选项长度的严格限制，为将来加入新选项提供更大的灵活性。

（4）流标签能力

为了满足发送者所要求的特殊处理，IPv6 增加了一个新的域来标记属于特殊传输数据流的数据包，如非默认的服务质量或实时业务等。

（5）认证和保密能力

IPv6 规定了包括认证、数据完整性和数据加密（可选）在内的扩展功能。

与 IPv4 相比，IPv6 具有以下几个优势。

① IPv6 具有更大的地址空间。

IPv4 中规定 IP 地址长度为 32，最大地址个数为 $2^{32}$；而 IPv6 中 IP 地址的长度为 128，即最大地址个数为 $2^{128}$。与 32 位地址空间相比，其地址空间增加了 $2^{128}-2^{32}$ 个。现在，IPv4 采用 32 位地址长度，约有 43 亿个地址，而 IPv6 采用 128 位地址长度，可以有无限制的地址，有足够的地址资源。地址的丰富将完全解除在 IPv4 互联网应用上的很多限制，如 IP 地址，每一个电话、每一个带电的东西都可以有一个 IP 地址，真正形成一个数字家庭。IPv6 的技术优势，目前在一定程度上解决了 IPv4 互联网存在的问题，这是 IPv4 向 IPv6 演进的重要动力之一。

② IPv6 使用更小的路由表。

IPv6 的地址分配一开始就遵循聚类的原则，这使得路由器能在路由表中用一条记录表示一片子网，大大减小了路由器中路由表的长度，提高了路由器转发数据包的速度。

③ IPv6 加入了对自动配置的支持。

这是对 DHCP 协议的改进和扩展，使得网络（尤其是局域网）的管理更加方便和快捷。

④ IPv6 具有更高的安全性。

在使用 IPv6 的网络中，用户可以对网络层的数据进行加密并对 IP 报文进行校验，IPv6 中的加密与鉴别选项提供了分组的保密性与完整性，极大地增强了网络的安全性。

⑤ 允许扩充。

如果需要新的技术或应用，IPv6 允许协议进行扩充。

⑥ 更好的头部格式。

IPv6 使用新的头部格式，其选项与基本头部分开，如果需要，可将选项插入到基本头部与上层数据之间。这就简化和加速了路由选择过程，因为大多数的选项不需要由路由选择。

## 3.2　IPv6 地址格式

IETF RFC 4291 规定了 IPv6 的地址格式。IPv6 地址是为接口或一组接口分配的一个 128 比特的标识符。IPv6 地址有下面三类。

- 单播地址：单一接口的标识符。发送到单播地址的分组被交付给由该地址标识的接口。
- 任播地址：一组接口（一般属于不同节点）的标识符。发送到任播地址的分组被交付给由该地址标识的一组接口之一（按照路由协议计算的距离中“最近的”一个）。
- 组播地址：一组接口的标识符（一般属于不同节点）。发送到组播地址的分组被交付给由该地址标识的所有接口。

IPv6 不使用广播地址，广播地址的功能由组播地址代替。

## 3.2.1 地址模型

所有类型的 IPv6 地址都分配给接口，而不是节点。IPv6 单播地址与单个接口对应，既然每个接口都属于一个单个节点，该节点的任何一个接口的单播地址可以当作该节点的一个标识符。

所有的接口都需要有至少一个链路本地单播地址。单个接口可能同时被分配任何类型或范围的多个 IPv6 地址。不作为任何 IPv6 数据包的源或目的的接口不需要超出链路范围的单播地址，这对于点到点接口来说有时是方便的，这种地址模型有一个例外：在执行中如果将多个物理接口当作一个来对待，当呈送给网络层时，可能会给多个物理接口分配一个单播地址或一组单播地址。这对于多个物理接口上的负载共享是有用的。

目前，IPv6 继承了 IPv4 的子网前缀与一个链路关联的模型。多个子网前缀可能属于同一条链路。

## 3.2.2 IPv6 地址的语法

IPv6 地址有三种通用形式。

首选形式是 x:x:x:x:x:x:x:x，在这里 x 是地址中的 8 个 16 进制的 16bit 块。如：

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

1080:0:0:0:8:800:200C:417A

地址的每个区中前面的零不需要写，但是每个区里至少要有一个数（下面的情况例外）。

由于分配不同类型 IPv6 地址的方法不同，通常地址中都会包含长串连续 0 位的情况。为便于书写这种地址形式，RFC 4291 中规定了专门的语法来压缩连续的 0 位，即用“：：”来代替连续的一组或多组 16bit 的 0 位。

但是“：：”在一个地址中只能出现一次，“：：”也可以用来代替地址中开头和末尾的连续 0 位。如下列地址：

1080:0:0:0:8:800:200C:417A 单播地址
FF01:0:0:0:0:0:0:101　　组播地址
0:0:0:0:0:0:0:1　　环回地址
0:0:0:0:0:0:0:0　　未指定地址

它们可以由下列形式代替：

1080::8:800:200C:417A　　单播地址
FF01::101　　组播地址
::1　　环回地址
::　　未指定地址

在既有 IPv6 节点又有 IPv4 节点的环境中，可以采用 x:x:x:x:x:x:d.d.d.d 的地址格式，其中“x”是十六进制的数值，用在地址的高位（6 个 16 位），“d”是十进制的数值，用在地址的低位（4 个 8 位）。例如：

0:0:0:0:0:0:13.1.68.3
0:0:0:0:0:FFFF:129.144.52.38

或者写成省略格式：

::13.1.68.3
::FFFF:129.144.52.38

## 3.2.3　地址前缀的语法

IPv6 地址前缀的语法类似于将 IPv4 的地址前缀写入 CIDR 符号中，IPv6 的地址前缀由下面的形式来表示：

IPv6 地址/前缀长度

其中，IPv6 地址是 2.2.2 节中任何形式表示的 IPv6 地址，前缀长度是一个十进制的数值，它表示地址中组成前缀的最左边相邻位的位数。

下例中给出 60bit 前缀 12AB00000000CD3（十六进制）的合法表示方法：

12AB:0000:0000:CD30:0000:0000:0000:0000/60
12AB::CD30:0:0:0:0/60
12AB:0:0:CD30::/60

而如下表示方法则是非法的：

12AB:0:0:CD3/60　　它可能会丢掉了前面的 0，而不是末尾的。

12AB::CD30/60“/”　左边的地址可能会被理解成这样的形式：12AB:0000:0000:0000:0000:000:0000:CD30。

12AB::CD3/60“/”　左边的地址可能会被理解成：12AB:0000:0000:0000:0000:000: 0000:0CD3。

当需要同时写一个节点地址和该节点地址的一个前缀（如该节点的子网前缀）

时，两者可以结合成下面的形式。

节点地址：12AB:0:0:CD30:123:4567:89AB:CDEF。

子网号：12AB:0:0:CD30::/60。

也可以省略为：12AB:0:0:CD30:123:4567:89AB:CDEF/60。

## 3.2.4 地址类型标识

地址中前导的比特位表示 IPv6 地址的类型，长度可变的前导比特位称作格式前缀，前缀的分配方法如表 3-1 所示。

表 3-1 地址前缀的分配方法

| 地址类型 | 二进制前缀 | IPv6 符号表示法 |
|---|---|---|
| 未指定 | 00…0（128 比特） | ::/128 |
| 环回 | 00…1（128 比特） | ::1/128 |
| 组播 | 11111111 | FF00::/8 |
| 链路本地 | 1111111010 | FE80::/10 |
| 全球单播 | 其他情况 | |

任播地址取自（具有任何范围的）单播地址空间，在句法上任播地址与单播地址难以区分。

出于其他考虑，将来的标准可以为全球单播空间重新定义细分的一种或多种子空间，但是，除非出现这种重新定义和直到这种重新定义发生，实现中必须把没有以上述列出的任何一种前缀开始的所有地址当作全球单播地址。

## 3.2.5 单播地址

IPv6 单播地址是连续的、以位为单位的可掩码地址，和带有 CIDR 的 IPv4 地址相似。

在 IPv6 中，有以下几种类形式的单播地址：全球单播地址、站点本地单播（已被废止）、链路本地单播。全球单播地址还有一些特定目的的子类型，如带有嵌入 IPv4 地址的 IPv6 地址。将来可以定义新增的地址类型或子类型。

IPv6 节点对 IPv6 地址的内部结构知道的可多可少，这取决于该节点的功能。最简单的情况下，一个节点可能把一个 IPv6 地址当成一个 128 位长的字符串，如图 3-1 所示。

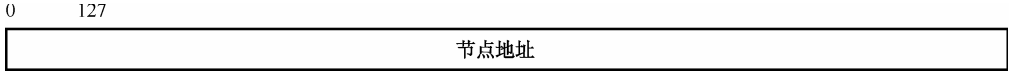



图 3-1 IPv6 地址的内部结构 1

稍微复杂的节点可能会通过表示子网的前缀来把 IPv6 地址结构分成两部分，由网络前缀和接口标识组成，如图 3-2 所示，不同的地址 *n* 可以有不同的值。

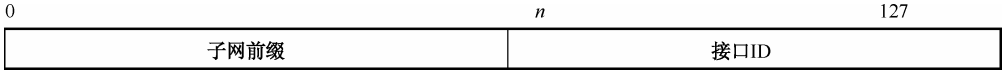



图 3-2　IPv6 地址的内部结构 2

单播地址中，更复杂的节点可以有其他的分级方式。路由器可以更为具体地了解一级或多级结构的边界。了解的程度取决于路由器在路由结构中所处的位置。

### 1．接口标识（Interface ID）

在 IPv6 单播地址中，接口标识用来分辨在一个链路中的多个接口。在同一子网前缀内它们必须是唯一的。建议不给同一链路上的不同节点分配相同的接口标识。在更广的范围内接口标识可能也是唯一的。在某些情况下，接口标识会直接从接口的链路层地址得来。在同一节点上，多个接口可以使用相同的接口标识，只要这些接口附着在不同的子网上即可。

值得注意的是，不同节点使用同一接口标识并不影响该接口的全球唯一性或使用该接口标识的每个 IPv6 地址的全球唯一性。

对于所有的单播地址来说，除了以二进制 000 开头的地址，其他情况下要求接口标识为 64 比特长，按改进的 EUI-64 格式构建。

当源自全球标记时（如 IEEE 802 48-bit MAC 或 IEEE EUI-64），基于改进的 EUI-64 格式的接口标识可以有全球范围；当不能得到全球标记时（如串联链路、隧道端点）或不希望使用全球标记时（如临时的私有标记），基于改进的 EUI-64 格式的接口标识可以有本地范围。

当根据 IEEE EUI-64 标识形成接口标识时，通过插入“u”比特（universal/local 比特，IEEE EUI-64 术语），即可形成改进的 EUI-64 格式接口标识。在改进的 EUI-64 格式中，“u”比特置 1 表示全球范围，“u”比特置 0 表示本地范围。二进制形式的 IEEE EUI-64 标识的前 3 字节如图 3-3 所示。

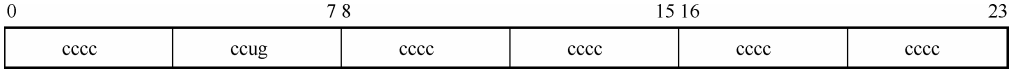



图 3-3　IEEE EUI-64 的二进制标识中前三个字节

图 3-3 是按照互联网标准的比特顺序书写的，其中“u”代表 universal/local 比特，“g”代表 individual/group 比特，“c”代表 company_id 比特。

IPv6 节点不需要去证实这种由改进的 EUI-64 标记（该标记的“u”比特设置为全球范围）生成的接口标识符是唯一的。

### 2. 未指定地址

地址 0:0:0:0:0:0:0:0 称为未指定地址，它不能被分配给任何节点。节点在初始状态如果不知道自身的地址，可以把它作为数据包的源地址。

未指定地址不能作为 IPv6 包头的目标地址，也不能用于 IPv6 包头中的路由头。路由器不能转发源地址为未指定地址的 IPv6 数据包。

### 3. 环回地址

单播地址 0:0:0:0:0:0:0:1 称为环回地址。节点可以用它来给自己发送 IPv6 数据包。它不能被分配给任何实际的物理接口，它被看作属于链路本地范围，可以被当作是虚拟接口（典型称作“环回接口”）的链路本地单播地址，该虚拟接口通向一个假想的链路，该链路和谁都不连通。

环回地址不能被用作 IPv6 数据包（这些数据包是从单个节点发送到该节点外面的）中的源地址。以环回地址为目的地地址的 IPv6 数据包不能被发送到节点之外，并且不能经由 IPv6 路由器转发。接口收到目的地为环回地址的数据包必须将其抛弃。

### 4. 全球单播地址

IPv6 全球单播地址的一般格式如图 3-4 所示。

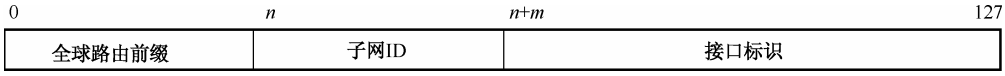



图 3-4　全球单播地址的一般格式

图 3-4 中，全球路由前缀是一个分配给站点（一群子网/链路）的值（典型上是层级结构的），子网 ID 是该站点内链路的标识符，接口标识的含义与前面的描述一致。

除了以二进制 000 开始的全球单播地址外，所有全球单播地址都有一个 64 位的接口标识字段（即 $n+m=64$）。以二进制 000 开始的全球单播地址在大小上或接口 ID 字段的结构上没有这类限制。

以二进制 000 开始的全球单播地址的例子是具有嵌入的 IPv4 地址的 IPv6 地址。

### 5. 内嵌有 IPv4 地址的 IPv6 地址

目前 IETF 定义了两类用于在地址的后 32 比特中携带 IPv4 地址信息的 IPv6 地址类型，分别是“IPv4 兼容 IPv6 地址”（IPv4-Compatible IPv6 Address）及“IPv4 映射 IPv6 地址”（IPv4-Mapped IPv6 Address）。

“IPv4 兼容 IPv6 地址”用于 IPv6 过渡。“IPv4 兼容 IPv6 地址”的格式如图 3-5

所示。

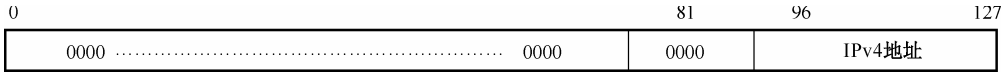



图 3-5　IPv4 兼容 IPv6 地址

在“IPv4 兼容 IPv6 地址”中使用的 IPv4 地址必须是全球唯一 IPv4 单播地址。“IPv4 兼容 IPv6 地址”现在已经过时，因为目前的 IPv6 过渡机制不再使用这些地址。因此，目前不再要求新的实现支持这种地址类型。

“IPv4 映射 IPv6 地址”用于将 IPv4 节点的地址表示为 IPv6 地址。“IPv4 映射 IPv6 地址”的格式如图 3-6 所示。

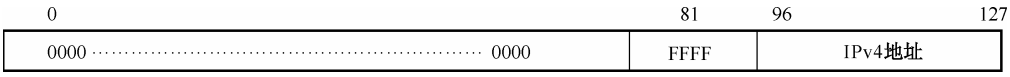



图 3-6　IPv4 映射 IPv6 地址

### 6. 链路本地 IPv6 单播地址

链路本地地址用于单一链路。链路本地地址格式如图 3-7 所示。

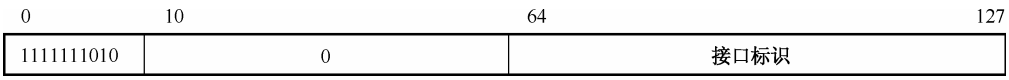



图 3-7　链路本地地址格式

链路本地地址被设计用于在单一链路上寻址，在诸如自动地址配置、邻居发现，或者在链路上没有路由器时使用。

路由器不能转发任何具有链路本地源地址或具有链路本地目的地地址的数据包到其他链路。

### 7. 站点本地 IPv6 单播地址

最初设计站点本地地址用于不需要全球前缀的站点内部寻址。现在，站点本地地址已经过时了。站点本地地址格式如图 3-8 所示。

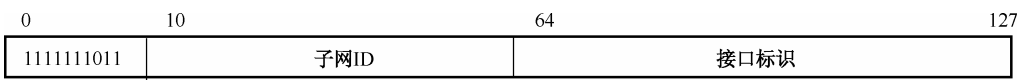



图 3-8　站点本地地址格式

在新的实现中，不能支持由 IETF RFC 3513 定义的这个前缀的特殊性质（即新的实现必须将此前缀看作全球单播）。

已有的实现和部署可以继续使用这个前缀。

### 3.2.6 任播地址

一个任播地址可以被同时分配给多于一个的属于不同节点的网络接口。其特点是以任播地址为目的地址的数据包会被转发到根据路由协议测量的距离最近的接口上。任播地址从单播地址中划分出来。可以使用任意已定义的单播地址格式。因此，任播地址从语法上无法与单播地址区分。当一个单播地址被配置在多个接口上时，该单播地址就变为任播地址，同时该节点必须被明确地配置以明白该地址是一个任播地址。

对任意已分配的任播地址，都有一个最长的地址前缀 P。该地址前缀标识了属于同一任播地址的所有接口所在的拓扑区域。在这个由 P 标识的区域中，任播地址的每个成员必须作为一个单独的个体在路由系统中进行广播（通常作为主机路由来进行引用）；而在该区域之外，该任播地址必须以地址前缀 P 而聚合到路由广播中去。

需要指出的是，在最坏的情况下，一个任播地址集合的地址前缀可能是一个空的前缀。也就是说，该集合的成员可能没有本地的拓扑区域。在这种情况下，该任播地址必须作为单独的路由项在整个因特网上广播。这样就对因特网该支持多少个这种“全球”性的任播地址提出了严格要求。因此，可以预料的是，对“全球”性任播地址的支持可能是不可行或非常严格的。

任播地址的一个预期应用是用来标识同属于一个因特网服务提供商的路由器集合。任播地址可以作为 IPv6 路由包头中的一种中间地址，用来强制该数据包经过某个特定的聚合或聚合系列而被转发。

任播地址的其他一些可能用途包括：标识那些连接在某个特定子网的路由器集合；标识提供到某个特定路由域的入口的路由器的集合。

子网路由器的任播地址是预定义的。其地址格式如图 3-9 所示。

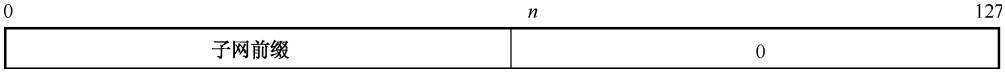



图 3-9 任播地址格式

任播地址中的子网前缀是指标识一个特定链路的前缀。此任播地址与该链路上的接口标识部分设为零的单播地址等同。

以子网路由器任播地址为目的地址的数据包会被转发到该子网的一个路由器上。所有路由器要求支持其所有接口所在子网对应的子网路由器任播地址。

提出子网路由器任播地址的目的是用于那些需要与一个远程子网中的路由器集合中的一个路由器进行通信的应用。

## 3.2.7　组播地址

一个 IPv6 的组播地址用于标识一组节点。一个节点可以属于多个组播地址组。组播地址具有如图 3-10 所示的格式。

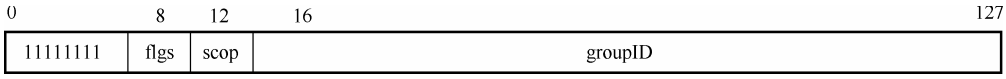



图 3-10　组播地址格式

该格式中起始的 11111111 表示该地址是一个组播地址。

标志域（flgs）中含四个标志: |0 |R |P |T|。

其中最高位的标志被预留，在初始化时需设置为零。

T 标志若为 0，则表示该地址是一个永久分配的（知名的）组播地址，由全球互联网权威组织统一分配；T 标志若为 1，则标识该地址是一个非永久分配的（临时的或动态分配的）组播地址。

P 标志若为 0，则表示该组播地址与网络前缀无关；P 标志若为 1，则表示该组播地址基于网络前缀分配，此时，T 标志必须设为 1。P 标志设为 1 时，组播地址的含义如图 3-11 所示。

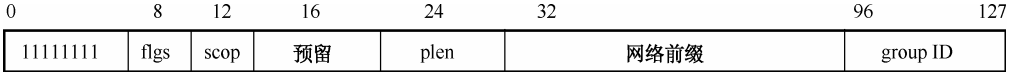



图 3-11　P 标志设为 1 时的组播地址格式

其中，plen 字段表示 network prefix 字段实际有效的比特数量。

网络前缀字段表示组播地址归属的单播子网的网络前缀，该字段中无意义的比特应设置为 0，该字段中的网络前缀最长为 64 比特。

R 标志若为 1，则表示该组播地址中嵌入了组播汇聚点（RP）的地址，此时，P、T 标志必须同时设置为 1，此时的组播地址前缀为 FF70::/12，图 3-12 中的 8 比特预留字段的后四位将被理解为嵌入的 RP 接口 ID。IETF RFC3956 规定了生成 RP 地址的方法，生成的 RP 地址如图 3-12 所示。

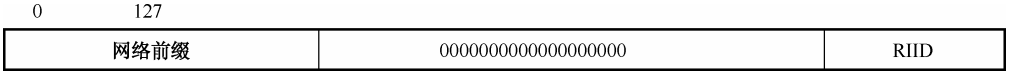



图 3-12　通过组播地址生成的 RP 地址格式

其中，网络前缀字段的值为图 3-11 中网络前缀字段的前“plen”比特，RIID 字段为图 3-11 中预留字段的后 4 比特。

长度为 4 比特的范围域（scop）决定该组播地址的有效范围。详细情况如下：

- 0 预留；

- 1 接口本地范围；
- 2 链路本地范围；
- 3 未分配；
- 4 管理本地范围；
- 5 站点本地范围；
- 6 未分配；
- 7 未分配；
- 8 组织本地范围；
- 9 未分配；
- A 未分配；
- B 未分配；
- C 未分配；
- D 未分配；
- E 全球范围；
- F 预留。

组标识域（group ID）用于在该地址的指定范围内永久性或临时性地标识该组播组。

永久分配的组播地址与该地址的有效范围是独立的。举例来说，如果“NTP 服务器组”被分配了一个永久组播地址，并且其组标识为 101，那么：

- FF01:0:0:0:0:0:0:101 表示与发送者处在同一节点的所有 NTP 服务器；
- FF02:0:0:0:0:0:0:101 表示与发送者处在同一链路的所有 NTP 服务器；
- FF05:0:0:0:0:0:0:101 表示与发送者处在同一站点的所有 NTP 服务器；
- FF0E:0:0:0:0:0:0:101 表示因特网上的所有 NTP 服务器。

非永久分配的组播地址只在指定范围内有意义。例如，在某个站点内的非永久组播地址 FF15:0:0:0:0:0:0:101，与其他站点内的具有相同地址的组播地址组没有任何关系，与组标识相同的但有效范围不同的非永久组播地址组也没有关系，与组标识相同的永久组播地址组也没有关系。

组播地址不能用在 IPv6 数据包的源地址域中，也不能出现在任何路由头中。

路由器不能转发超出在目的地组播地址中 scop 字段标识范围的任何组播数据包。

节点不能生成到 scop 字段包含保留值 0 的组播地址的数据包；如果收到这样的数据包，节点应将其丢弃。节点不能生成到 scop 字段包含保留值 F 的组播地址的数据包，如果发送或收到这样的数据包，该数据包的处理方式必须与包含全球（scop 字段为 E）组播地址的数据包一样。

以下是预定义的知名组播地址。

预留的组播地址：

FF00:0:0:0:0:0:0:0

FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

以上是预留的组播地址。这些地址绝不能分配给任何组播组。

① 所有节点地址：

FF01:0:0:0:0:0:0:1
FF02:0:0:0:0:0:0:1

以上组播地址标识所有 IPv6 节点组。有效范围分别为接口本地范围或链路本地范围。

② 所有路由器地址：

FF01:0:0:0:0:0:0:2
FF02:0:0:0:0:0:0:2
FF05:0:0:0:0:0:0:2

上述组播地址标识所有 IPv6 的路由器地址组，有效范围分别为接口本地范围、链路本地范围或站点本地范围。

③ 请求节点地址：

FF02:0:0:0:0:1:FFXX:XXXX

该组播地址作为节点的单播和任播地址的功能而计算。该地址由两部分组成：一部分取该地址（单播或任播）的低 24 比特，并拼接到前缀 FF02:0:0:0:0:1:FF00::/104 后面，一共 128 比特，组成一个组播地址。该地址范围是从 FF02:0:0:0:0:1:FF00:0000 到 FF02:0:0:0:0:1:FFFF:FFFF。例如，与地址 4037::01:800:200E:8C6C 相对应的请求节点组播地址为 FF02::1:FF0E:8C6C。这样对那些由于不同地址聚合需要、只是高位不同的 IPv6 地址将会映射到相同的请求节点地址。从而减少了节点必须加入的组播地址。

节点必须针对其被分配的每个单播和任播地址都计算并加入相应的请求节点组播地址。

## 3.3 IPv6 包头格式

IPv6 包头格式如图 3-13 所示。

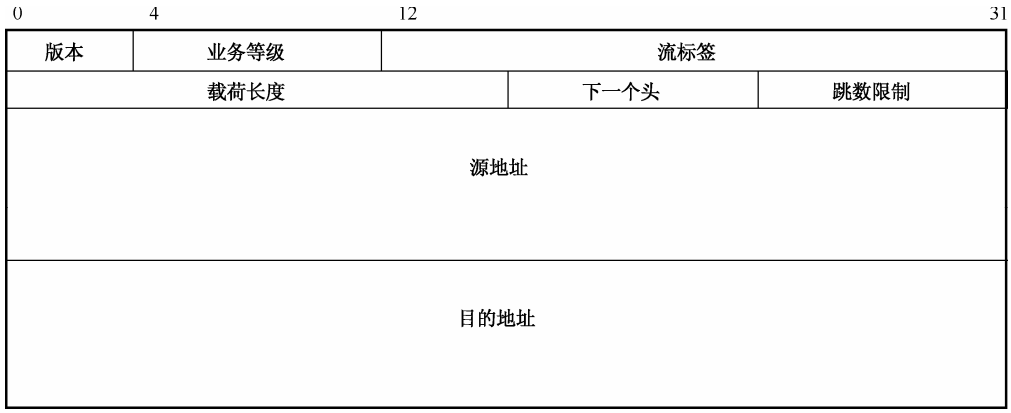



图 3-13　IPv6 包头格式

包头中各域的含义如下。

- 版本（Version）：该域长度为 4 比特，IPv6 版本号=6。
- 业务等级（Traffic Class）：该域长度为 8 比特。参见第 9 章。
- 流标签（Flow Label）：该域长度为 20 比特。参见第 8 章。
- 载荷长度（Payload Length）：该域为 16 比特无符号整数，表示 IPv6 载荷长度，即数据包中 IPv6 头之后其余部分的长度，以字节为单位。（注：任何扩展头都被认为是载荷的一部分，其长度应被计算在内。）
- 下一个头（Next Header）：该域长度为 8 比特，表示紧接在 IPv6 头后面的下一个头的类型。这个域取不同的值，对应的扩展头类型不同，值与扩展头类型之间的对应关系参见“IANA 协议号与指派服务网页”。
- 跳数限制（Hop Limit）：该域为 8 比特无符号整数，数据包每向前经过一个转发节点，跳数限制减 1，当跳数限制减至 0 时，该数据包被丢弃。
- 源地址（Source Address）：该域长度为 128 比特，表示产生数据包的节点的 IPv6 地址。
- 目的地址（Destination Address）：该域长度为 128 比特，表示期望数据包到达的 IPv6 地址，如果出现路由头，这个地址可能不是最终的接收数据包的 IPv6 地址。

### 1. IPv6 数据包的长度

IPv6 要求互联网中任何一条链路的 MTU 不小于 1280 字节。在任何一条不支持 1280 字节数据包的链路上，必须在 IPv6 层以下的一层提供与链路相关的分段和重组功能。

可配置 MTU 的链路必须将 MTU 配置为至少 1280 字节，建议这样的链路将 MTU 配置为 1500 字节或更高，以便在不进行分段的情况下适应可能出现的更大的数据封装。

在与某一节点直接相连的任一条链路上，这个节点必须能接收同这些链路的 MTU 一样大的数据包。

IPv6 强烈建议节点实现“路径 MTU 发现”，以便发现和利用具有大于 1280 字节的 MTU 的路径。然而，一个最简单的 IPv6 实现可以简单地限制自己不发送大于 1280 字节的数据包，从而省去了“路径 MTU 发现”。

为了能发送大于路径 MTU 的数据包，节点必须在数据源用 IPv6 分段头给数据包分段，并且在目的地进行重组。然而，如果应用能调节它的数据包使其适应路径 MTU，则不鼓励使用分段（即最小为 1280 字节）。

一个节点必须能接收重组后大小为 1500 字节的分段数据包。一个节点允许接收重组后大小为 1500 字节以上的分段数据包。一个依赖于 IPv6 分段来发送长度超过路径 MTU 的数据包的上层协议或应用不应该发送长度超过 1500 字节的数据包，除非它明确知道目的地节点有能力重组这么大的数据包。

当一个 IPv6 数据包被发送到 IPv4 目的地时，起始的 IPv6 节点可能会收到一个 ICMP“数据包过大”消息来报告下一跳的 MTU 小于 1280 字节。在这种情况下，并不要求 IPv6 节点把以后发送的数据包长度减少到 1280 字节以下，但必须在这些数据包中加入分段头，使承担 IPv6-IPv4 协议翻译的路由器能得到一个合适的标记值来进行 IPv4 的分段。注意，这意味着载荷长度可能会减少到 1232 字节（1280 减去 IPv6 头的 40 字节和分段头的 8 字节），如果有附加的扩展头存在，载荷长度可能还会更少。

### 2. 流标签

IPv6 头内的流标签域占 20 比特，源节点用它来标记那些需要 IPv6 路由器特殊处理的一系列数据包，这些特殊处理包括“非默认的服务质量”或“实时服务”。有关这方面的内容在 IPv6 制定时还处于试验阶段，随着互联网的发展方向不断明朗，支持流的要求会使这部分内容得到更改。对于那些不支持流标签域功能的主机和路由器来说，当发送一个数据包时，在这个域填入 0 值；当转发数据包时，对这个域不作任何改动；当接收数据包时，忽略这个域。

一个流是指从一个特定的源地址到特定的目的地址（单播或组播地址）发送的一组数据包，并且源节点希望中间的路由器对流进行特殊的处理。这种特殊处理的属性可以通过控制协议传到路由器（如资源预留协议），或者通过流数据包本身所携带的信息传到路由器（如逐跳选项）。这样的控制协议或选项的详细内容不在本标准讨论范围内。

一对源和目的之间有可能有多个激活的流，也可能有不属于任何一个流的流量。一个流由源地址和非 0 流标签的组合唯一确定。不属于任何一个流的数据包的流标签为 0。

一个流的流标签由流的源节点指定。新的流标签必须从 1～0xFFFFF（十六进制）范围内（伪）随机并且唯一地选择。随机分配的目的是使所产生的流标签的任何一组比特都能作为路由器中哈希表的键值，这个键值用于查找流对应的状态。

所有属于同一个流的数据包发送时必须具有相同的源地址、目的地址和流标签。如果其中任何一个数据包包含逐跳选项头，那么流的每一个包都必须包含相同的逐跳选项头（逐跳选项头中的下一个头域除外）。如果其中任何一个数据包包含路由头，那么流的每一个包都必须包含相同的路由头并包括路由头的扩展头（路由头中的下一个头域除外）。允许但并不要求路由器或目的节点检证这些条件是否满足。如果检测到条件不满足的数据包，应当向源节点发送 ICMP 参数错误消息，消息代码为 0，消息指针指向流标签的高位字节（即 IPv6 包的第二字节）。

沿着流路径建立的流处理状态的最大生存周期必须在状态建立机制中说明，如资源预留协议或建立流的逐跳选项。源节点不允许在任何流处理状态的最大生存周期内把该流标签分配给新的流，因为在使用流标签前，可能状态已经建立起来了。

当一个节点重启时（如死机后的恢复运行），必须小心使用流标签，因为该流标签有可能在前面的仍处于最大生存周期内的流中使用。这可以通过在静态存储上记录流标签的使用情况来实现，从而在死机恢复后仍然保存该信息，或者避免在任何先前可能建立的流的最大生存周期过期之前使用任何流标签。如果节点的最小重启时间已知，实际重启时间可以从等待分配流标签所需的时间中推算得到。

不要求所有或至少大多数数据包属于某一个流，即都带有非 0 的流标签。这条规则提醒协议设计者和实现者不要做相反的假设。例如，只有在大部分数据包都属于流时路由器性能良好；或者路由器的包头压缩机制只处理属于流的数据包，这种设计路由器的方法都是不合理的。

### 3. 业务等级

IPv6 头中的 8 比特业务等级域被源节点和/或路由器用于确定 IPv6 数据包的等级或优先权。目前在 IPv4 中正在试验使用业务类型域为 IP 数据包提供不同形式的区分服务，IPv6 头中的业务等级域与此具有类似的功能。

下面列出了一些对业务等级域的通用要求。

- IPv6 服务接口必须能为上层协议提供一种方法，使之在生成数据包时可以修改业务等级域的值。该域的默认值为 0。
- 支持业务等级域的特殊应用的节点可以在生成、转发或接收数据包时根据特殊应用的需要改变这一域的值。不具备此能力的节点应忽略此域并且不能对其进行修改。
- 一个上层协议接收到的数据包中的业务等级域的值与源节点发送的数据包中该域的值可能不同。

### 4. IPv6 扩展头

在 IPv6 中，可选择的互联网层信息被编码在单独的头中，并放在一个数据包内的 IPv6 头和上一层头之间。这种扩展头的数量不多，每个扩展头都被一个明确的“下一个头”域的值所确定。如图 3-14 所示，每个 IPv6 数据包可带有 0 个、1 个或多个扩展头，每个扩展头由前一个头的“下一个头”域所确定。

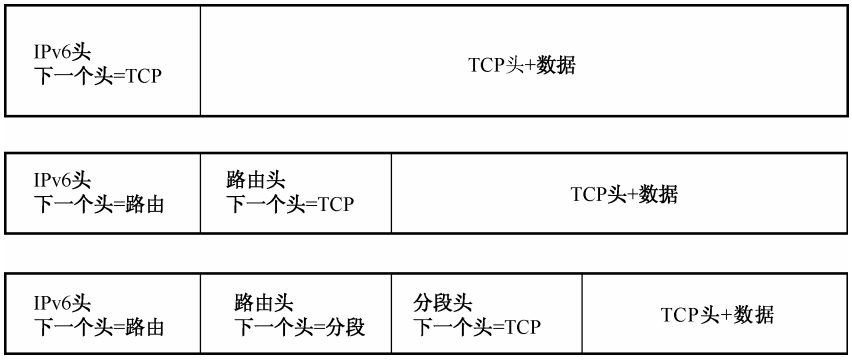



图 3-14　IPv6 扩展头

除了逐跳选项头之外的其他扩展头不被数据包发送路径上的任何一个节点检查或处理，除非数据包到达了 IPv6 头中“目的地址”域所指明的节点（或在组播路由的情况下，节点组中的任一个节点）。在 IETF RFC 7045 中定义了一种例外情况，如果转发节点出于某种目的（如防火墙）需要检查扩展头，那么该节点就应该能够识别并处理 IETF 已经定义过的扩展头。IETF RFC 2460 中要求目的节点丢弃包含未知扩展头的数据包，但是，中间的转发节点不能这么做，这是由于这种未知扩展头有可能是新近定义的，而中间节点的实现此时尚未升级更新。中间节点只能依据预配置的策略丢弃一个数据包，而不能因为它包含未知的扩展头而丢弃它。中间节点必须能够被配置为允许转发包含未知扩展头的数据包，而默认的配置则可以是丢弃这样的数据包。

在对 IPv6 头中“下一个头”域正常解复用时，首先要处理第一个扩展头（没有

扩展头时直接处理上层头）。每一个扩展头的内容和语义决定了是否要继续处理下一个头。因此，必须严格按照扩展头在数据包中出现的顺序对它们进行处理。接收者不能在数据包中搜索一个特定的扩展头，并且在处理完所有排在它前面的头之前处理它。

逐跳选项头中携带的信息必须被数据包传送路径上包括源节点和目的节点在内的每一个节点检查和处理。但是，某些高性能路由器为了提高转发效率，可能会忽略逐跳选项头或将包含该头的数据包放入低优先级队列中处理。逐跳选项头如果存在，则它必须紧随在 IPv6 头之后。当 IPv6 头中“下一个头”域的值为 0 时，说明后面有逐跳选项头存在。

如果节点处理一个头的结果是要进行下一个头的处理，但这个头的“下一个头”域的值不能被节点所识别，则节点将丢弃这个数据包并向数据包的源节点发送一个 ICMP“参数错误”消息，ICMP 代码值为 1（不能识别下一个头的类型），ICMP 指针域包含源数据包中不能被识别的域的偏移量。若一个节点遇到除 IPv6 头以外的任一个头的“下一个头”域为 0，则节点对这个数据包也应按上面的方法进行处理。

每个扩展头的长度应为 8 的整数倍（以字节为单位），以保证下面的头也按 8 字节对齐。每个扩展头内的多字节域按它们的自然分界来对齐。

IPv6 的完整实现包括下面扩展头的实现：

- 逐跳选项；
- 路由；
- 分段；
- 目的地选项；
- 认证（注 1，注 3）；
- 封装安全载荷（注 2，注 3）。

注 1：认证头用于为 IP 数据报提供无连接完整性和数据初始认证，此外还能防止重发攻击的发生。

注 2：封装安全载荷头用于提供机密性、数据初始认证、无连接完整性，防止重发攻击及受限的数据流机密性。

注 3：认证头和封装安全载荷头可以结合使用，也可以通过使用隧道模式嵌套使用。它们可以在主机之间、安全网管之间或安全网管与主机之间提供安全服务。封装安全载荷头还可以提供机密性（加密）服务。它们之间的主要区别在于覆盖的范围不同。此外，如果 IP 头不通过封装安全载荷头来封装（以隧道模式），那么封装安全载荷头将不会保护任何 IP 头中的域。

（1）扩展头的顺序

当一个数据包中使用多个扩展头时，这些头应按照下面的顺序出现：

- IPv6 头；

- 逐跳选项头；
- 目的地选项头（注 1）；
- 路由头；
- 分段头；
- 认证头（注 2）；
- 封装安全载荷头（注 2）；
- 目的地选项头（注 3）；
- 上层头。

注 1：这些选项要在 IPv6 目的地址域所列出的第一个目的地进行处理，也要在路由头所列出的后续目的地进行处理。

注 2：在 IETF RFC 1827 中给出了有关认证头和封装安全载荷头之间的相对顺序的附加建议。

注 3：这些选项只在数据包的最终目的地进行处理。

同一类型的扩展头最多只能出现一次（如果有多个同种扩展头，它们应顺次连续排列在一起），唯一例外的是目的地选项头可以出现两次：一次在路由头前出现，另一次在上层头前出现。

如果上层头是另一个 IPv6 头（即 IPv6 通过隧道方式封装在 IPv6 中），那么接在它后面的是它自己的扩展头，这些扩展头也应按照上面规定的顺序来排列。

如果要定义其他扩展头，则必须说明它们同以上所列的头的顺序约束关系。

IPv6 的节点必须接受并处理同一个数据包中以任何顺序、任何次数出现的扩展头，只有逐跳选项头才必须严格地接在 IPv6 头之后。然而，我们强烈建议数据包的发送者严格遵守上面建议的顺序，除非以后的规范推翻这一顺序。

（2）选项

在前面介绍的扩展头中，逐跳选项头和目的地选项头可携带不定数量的选项。这些选项采用 TLV 编码方式，格式如图 3-15 所示。

| 选项类型 | 选项数据长度 | 选项数据 |
|---|---|---|

图 3-15　IPv6 扩展头中的选项格式

选项类型（Option Type）：无符号的 8 位整数，说明选项的类型。

选项数据长度（Opt Data Len）：无符号的 8 位整数，以字节为单位，表示选项数据的长度。

选项数据（Option Data）：是个可变长度域，包含“选项类型”的数据。

接收者在处理一个头时，必须严格按照每个选项在头中出现的顺序来处理它们。例如，不能在头中搜索一个选项并在处理排在它前面的选项之前处理它。

在内部编码时，“选项类型”域的最高位两比特指明了当 IPv6 节点不能识别该

选项类型时所必须采取的动作：

00——跳过这个选项并继续处理该头；

01——丢弃这个数据包；

10——丢弃这个数据包，并且无论这个数据包的目的地址是否是组播地址，都向该数据包的源地址发送一个 ICMP 数据包，指出不能识别的选项类型；

11——丢弃这个数据包，并且只有当目的地址不是组播地址时，向该数据包的源地址发送一个 ICMP“参数错误”消息，代码值为 2，指针域指向不能识别的选项类型。

“选项类型”域的第三位指明这个选项的数据是否能改变数据包到达最终目的地的路由。当一个数据包中有认证头时，对于选项数据可能改变选路的任何选项，在计算或验证数据包的认证值时，这个选项的整个数据域必须当作 0 值来处理。

0——选项数据不改变选路；

1——选项数据可能改变选路。

上述的三个高位比特应被视为选项类型的一部分，而不应独立于选项类型。也就是说，应由一个完整的 8 比特选项类型来标识一个特别的选项，而不能仅由选项类型的低位 5 个比特来标识。

逐跳选项头和目的地选项头都使用相同的选项类型编号空间。然而，一个特别的选项可能会被限制只能用于这两个头中的一个。

个别的选项有特殊的对齐要求，以确保选项数据域中的多字节值符合自然分界。一个选项的对齐要求是用 xn+y 表示的。也就是说，选项类型必须是在从该扩展头开始算的 x 字节的整数倍加上 y 个字节的位置出现。

例如：

2n　　指从该扩展头开始的任何 2 字节偏移。

8n+2　　指从该扩展头开始的任何 8 字节偏移，加上 2 字节。

有两类填充选项，当需要时用于后续选项的排列，以填充该头，使其长度为 8 字节的整数倍。所有 IPv6 节点必须能识别这些填充选项。

（3）逐跳选项头

逐跳选项头用来携带那些在数据包发送路径上必须由每个节点检查的信息。如果 IPv6 头的“下一个头”域的值为 0，则说明紧接着 IPv6 头的下一个头是逐跳选项头。

逐跳选项头的格式如图 3-16 所示。


图 3-16　逐跳选项头的格式

下一个头（Next Header）：该域长度为 8 比特，定义紧接在逐跳选项头之后的头的类型。这个域取不同的值，对应的扩展头类型不同，值与扩展头类型之间的对应关系参见“IANA 协议号与指派服务网页”。

扩展头长度（Hdr Ext Len）：该域是一个 8 比特无符号整数，以 8 字节为单位，表示逐跳选项头的长度，它不包括起始的 8 字节。

选项（Options）：该域长度可变，其长度应保证整个逐跳选项头的长度为 8 字节的整数倍长，包含有一个或多个 TLV 编码的选项。

目前只为逐跳选项头规定了 Pad1 和 PadN 选项。

（4）路由头

IPv6 源数据包使用路由头来列出数据包从源地址到目的地址之间需要访问的一个或多个中间节点。该功能非常类似于 IPv4 的松散源选项和记录路由选项。如果某一个头的“下一个头”域值为 43，则说明紧接着它的下一个头是路由头。

路由头的格式如图 3-17 所示。

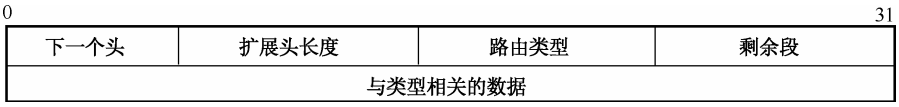



图 3-17　路由头的格式

下一个头（Next Header）：该域长度为 8 比特，定义紧接在路由头之后的头的类型。这个域取不同的值，对应的扩展头类型不同，值与扩展头类型之间的对应关系参见“IANA 协议号与指派服务网页”。

扩展头长度（Hdr Ext Len）：该域为 8 比特无符号整数，以 8 字节为单位，表示路由头的长度，不包括起始的 8 字节。

路由类型（Routing Type）：该域长度为 8 比特，标识不同类型的路由头。

剩余段（Segments Left）：该域为 8 比特无符号整数，表示剩余的路由段的数量，即在到达最终目的节点之前已经列出但尚未访问的中间节点的数目。

与类型相关的数据（Type-Specific Data）：该域长度可变，格式由“路由类型”决定，长度应保证整个路由头的长度是 8 字节的整数倍。

节点在处理接收到的数据包时，如果遇到一个路由头包含有不能识别的“路由类型”值，则节点要依据“剩余段”域的值采取措施。具体方法如下所述。

① 如果“剩余段”的值为 0，则节点忽略这个路由头，继续处理数据包中的下一个头（其类型由路由头的“下一个头”域的值标识）。

② 如果“剩余段”的值不为 0，则节点必须丢弃这个数据包，并且向数据包的源地址发送一个 ICMP“参数错误”消息（代码值为 0），ICMP 指针指向不能识别的“路由类型”。

如果一个中间节点在处理完接收数据包的路由头后，决定应将该数据包转发到一条链路 MTU 小于该包长度的链路上，那么该节点必须丢弃此数据包并向该包的源地址发送一个 ICMP“数据包过大”消息。

（5）分段头

IPv6 源节点使用分段头来发送数据包长度比路径 MTU 大的数据包。如果一个头的“下一个头”域的值为 44，则说明紧接在它后面的一个头是分段头。

分段头的格式如图 3-18 所示。


图 3-18　分段头的格式

下一个头（Next Header）：该域长度为 8 比特，定义紧接在路由头之后的头的类型。这个域取不同的值，对应的扩展头类型不同，值与扩展头类型之间的对应关系参见“IANA 协议号与指派服务网页”。

保留域（Reserved）：该域长度为 8 比特，传输时初始值设为 0，接收方忽略此域。

分段偏移（Fragment Offset）：该域长度为 13 比特，以 8 字节为单位，表示该头后面的数据相对于原始数据包可分段部分的起始位置的数据偏移量。

保留（Reserved）：该域长度为 2 比特，传输时初始值设为 0，接收方忽略此域。

标志位 M（M Flag）：该域长度为 1 比特，M=1 表示还有更多的分段，M=0 表示这是最后一段。

标识（Identification）：该域长度为 32 比特，详述如下。

为了从源节点传送一个大于路径 MTU 的数据包到目的节点，源节点可将该数据分段，并将每个分段作为一个独立的数据包传送，由接收者重新进行组装。

IPv6 节点在发送需要分段的数据包时，一定不能生成重叠的分段，接收节点在进行重组时，如果发现重叠的分段，则该节点应丢弃所有相关的数据包。

源节点为每个要分段的数据包生成一个标识值。该标识值必须不同于从相同源地址到相同目的地址的最近（注）发出的任何其他数据包的标识值。如果有路由头存在，则上述目的地址指的是最终目的地址。

注：“最近”是指在一个包的最大可能生存时间内，包括从源到目的地的传输时间和等待同一个数据包的其他分段重新组装的时间。然而，源节点并不需要知道数据包的最大生存时间。可以假定满足这种要求的方法是把该标识值作为一个 32 位的循环计数器使用，一旦有数据包被分段，该计数器就增加 1，并填入“标识”域。用这种方法来保证“标识”的唯一性。对于每个 IPv6 实现，它可以自己决定是配置

单独的节点计数器，还是配置多个计数器，即给每个可能的源地址配置一个计数器，或是给每一对源地址和目的地址配置一个计数器。

原始数据包是指最初的、没有分段的数据包，它由下面两部分组成。

原始数据包样式如图 3-19 所示。

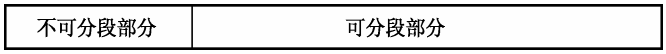



图 3-19　原始数据包样式

不可分段部分包括 IPv6 头及到达目的地路径上由节点处理的所有扩展头，如所有头包括路由头或逐跳选项头（如果有的话），不然就是没有扩展头。

可分段部分包括该数据包余下的部分，其中包括只能由目的节点处理的扩展头、上层头和数据。

原始数据包的可分段部分被分成段，除了最后一段外，每一段的长度都应是 8 字节的整数倍。每一个分段数据包按如图 3-20 所示的方式传输。


图 3-20　数据包分段实例

每个分段数据包的组成如下。

① 源数据包的不可分段部分，其中源 IPv6 头内的载荷长度改为该分段数据包的长度（不包括 IPv6 头本身的长度），并且将不可分段部分的最后一个头的下一个头域值改变为 44。

② 分段头部分。

- 下一个头（Next Header）：标识原始数据包可分段部分的第一个头。
- 段偏移（Segments Left）：以 8 字节为单位，表示分段相对于原始数据包可分段部分开始位置的偏移量，第一个分段的段偏移域的值为 0。
- 标志位 M（M Flag）：M=0 表示该分段是最后一段，M=1 表示该分段不是最后一段。
- 标识（Identification）：用来标识原始数据包。

③ 分段本身。

分段数据包的长度必须不能超过到数据包目的地路径的路径 MTU。

在目的节点，要对分段数据包重新进行组装以恢复成原始未分段时的形式。

重组后的原始数据包如图 3-21 所示。


图 3-21　重组后的原始数据包

以下是重组时应遵循的原则。

一个原始数据包只能由具有相同源地址、目的地址和分段标识的分段数据包来重组。

重组数据包的不可分段部分包括所有头但不包括第一个分段数据包的分段头，它主要做如下两个改动。

- 不可分段部分最后一个头的“下一个头”域的值取自第一个分段的分段头的“下一个头”域；
- 重组数据包的载荷长度从不可分段部分的长度、最后一个分段的长度和偏移量计算得来。计算重组的源数据包长度的公式为：

PL.orig=PL.first-FL.first-8+（8*FO.last）+FL.last

式中：

PL.orig=重组数据包的载荷长度值；

PL.first=第一个分段数据包的载荷长度值；

FL.first=第一个分段数据包中分段头后面的分段的长度；

FO.last=最后一个分段数据包中分段头的“段偏移”的值；

FL.last=最后一个分段数据包中分段头后面的分段的长度。

重组数据包的可分段部分是由每个分段数据包的分段头后面的分段组成的。每个分段的长度等于数据包载荷长度减去 IPv6 头与分段本身之间的头的长度，每个分段在数据包“可分段部分”中的相对位置由“段偏移”的值计算而来。

分段头不出现在最终的重组数据包中。

下面的错误情况可能会在重组分段数据包时发生：如果在接收到第一个到达的分段之后的 60s 内，一个数据包所有要重组的分段没有全部到达，需放弃重组该数据包，并且所有已接受的分段都要丢弃。在这种情况下，如果第一个分段数据包已接收到，则要向那个分段数据包的源地址发送一个 ICMP“超时-段重组超时”消息。

如果从分段数据包“载荷长度”域中得到的分段长度不是 8 字节的整数倍，并且这个段的 M 标志位是 1，则这个段必须丢弃，并且要向段的源地址发送一个 ICMP“参数错误”消息（代码为 0），ICMP 指针指向分段数据包的“载荷长度”域。

如果一个分段的长度和偏移导致出现这种情况，即由这个分段重组的数据包“载荷长度”超过 65535 字节，则必须丢弃这个分段，并且向分段的源地址发送一个 ICMP“参数错误”消息（代码为 0），ICMP 指针指向分段数据包的“段偏移”域。

下面的几种情况，虽然不希望在重组时出现，但在发生时不认为是错误的。

同一个数据包的不同分段的分段头，在其前面的头的个数和内容可以不同。无论什么头，只要出现在每个分段数据包的分段头前，则当数据包到达时，都要在重组排队之前被处理。只有那些偏移量为 0 的分段数据包的头才保留在重组数据包中。

同一个原始数据包的不同分段的分段头的“下一个头”的值可以不同。因为只有偏移量为 0 的分段数据包的相应值才在重组时有用。

（6）目的地选项头

目的地选项头用来携带只需由目的节点处理的选项信息。当某一个头的“下一个头”域的值为 60 时，说明紧接在这个头后面的头是目的地选项头。它的格式如图 3-22 所示。

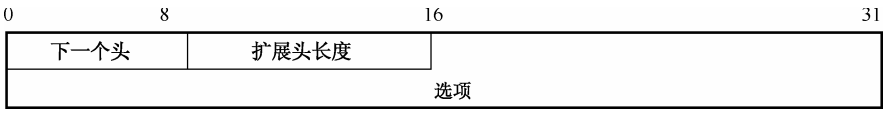



图 3-22　目的地选项格式

下一个头（Next Header）：该域长度为 8 比特，定义紧接在目的地选项头之后的头的类型。这个域取不同的值，对应的扩展头类型不同，值与扩展头类型之间的对应关系参见“IANA 协议号与指派服务网页”。

扩展头长度（Hdr Ext Len）：该域是一个 8 比特无符号整数，以 8 字节为单位，表示目的地选项头的长度，它不包括起始的 8 字节。

选项（Options）：该域长度可变，其长度应保证整个目的地选项头的长度为 8 字节的整数倍长，包含有一个或多个 TLV 编码的选项。

目前只为“目的地址选项”头规定了 Pad1 和 PadN 选项。

注意，在 IPv6 数据包中可以用两种方式来把可选择的目的地信息进行编码：作为目的地选项头的一个选项，或是作为单独的扩展头。分段头和认证头是后一种方式的例子。具体采用哪种方式要根据不能识别可选信息的目的节点希望采取的动作而定。

① 如果目的地节点希望采取的动作是丢弃数据包，并且只有当数据包目的地地址不是组播地址时，向数据包的源地址发送一个 ICMP“不能识别类型”消息，然后信息可以作为单独的头或作为目的地选项头的一个选项（“选项类型”域的高位两比特的值为 11）来进行编码。具体选用哪种方式的准则是使用的字节数少，或是排列容易，或者语义解析时更有效。

② 如果希望采取其他动作，则信息必须作为目的地选项头的一个选项（“选项类型”域的高位两比特的值为 00、01 或 10）来进行编码。

（7）无下一个头

IPv6 头或任何扩展头中“下一个头”域的值为 59 表示这个头后面没有任何数据

了。如果 IPv6 头的“载荷长度”域指出头后还有字节，而这些字节与在一个包含 59 值的头后面，则必须忽略这些字节，同时，如果该数据包是转发的，则保持不变，继续传送。

# 3.4 IPv6 基础协议

## 3.4.1 IPv6 邻居发现协议

节点（主机和路由器）使用邻居发现来确定相连链路上邻居的链路层地址，并迅速删除无效的缓存值。主机也使用邻居发现来寻找进行包转发的邻居路由器。另外，节点使用邻居发现机制，可以主动跟踪哪些邻居是可达的或者是不可达的，并检测改变的链路层地址。当路由器或到达路由器的路径发生故障时，主机主动寻找正在工作的另一个路由器或另一条路径。

IPv6 的邻居发现协议和 IPv4 的 ARP、ICMP 路由器发现和 ICMP 重定向相对应，在 IPv4 中没有相应的邻居不可达检测机制和协议。

邻居发现支持的链路类型有：点到点、组播、NBMA、共享介质、可变 MTU、不对称可达性。

### 1. 邻居发现机制的功能

邻居发现机制具有以下功能。

- 路由器发现：主机怎样定位相连链路上的路由器。
- 前缀发现：主机怎样发现一组地址前缀，这些前缀定义了哪些目的地在相连链路上是在连接的（on-link）。
- 参数发现：节点怎样了解发送接口的链路参数（如链路 MTU）或网络参数（如跳数限制值）。
- 地址自动配置：节点怎样自动配置接口的地址。
- 地址解析：在给出目的地 IP 地址的情况下，节点怎样确定在连接（on-link）目的地（如邻居）的链路层地址。
- 下一跳确定：将目的地 IP 地址映射成邻居 IP 地址的算法，下一跳可以是路由器或目的地。
- 邻居不可达检测：节点怎样确定邻居不可达。如果邻居是路由器，可以使用默认路由器；如果邻居既是路由器又是主机，需要再执行地址解析。
- 重复地址检测：节点怎样确定将要使用的地址没有被另一个节点正在使用。
- 重定向：路由器怎样通知主机到达目的地的最佳下一跳。

### 2. 邻居发现定义 ICMP 包类型

邻居发现定义了五种不同的 ICMP 包类型：路由器请求和路由器通告消息、邻居请求和邻居通告消息、重定向消息。

（1）路由器请求

当接口工作时，主机立即发送路由器请求消息，要求路由器产生路由器通告消息，而不必等待下一个预定时间。

（2）路由器通告

路由器周期性地通告它的存在及配置的链路和网络参数，或者对路由器请求消息作出响应。路由器通告消息包含连接（on-link）确定、地址配置的前缀和跳数限制值等。

路由器发现是基本协议的一部分，主机不必探测路由协议。

在组播链路上，每个路由器周期地组播路由通告包，来通告它的可用性。主机从所有路由器接收路由器通告，建立默认路由器列表。路由器频繁地产生路由器通告，以使主机在几分钟内了解它的可用性，也可单独使用邻居不可达检测算法进行故障检测。

路由器通告包含用作在连接（on-link）确定和/或地址配置的前缀列表，以及表明特定前缀用途的前缀标志位。主机使用通告的，在连接（on-link）前缀建立和维护列表，列表用来决定包的目的地是在连接（on-link）还是在路由器外。即使目的地不包含在被通告的在连接（on-link）前缀中，目的地也可以是在连接。在这种情况下路由器发送重定向消息，来通知发送者目的地是一个邻居。

路由器通告允许路由器通知主机如何执行地址配置。例如，路由器能指示主机是使用状态地址配置还是使用无状态地址配置。

路由通告消息包含网络参数，如主机的发送接口使用的跳数限制值等，包含可选的链路参数，如链路 MTU。这样有利于集中管理这些设置在路由器上的重要参数，并能自动传送到所有相连的主机上。

路由器通告含有链路层地址，不需要另外的包交换来解析路由器的链路层地址；含有链路前缀，不需要单独的机制配置掩码。

路由器通告链路上主机使用的 MTU，保证链路上所有节点使用相同的 MTU 值。

（3）邻居请求

节点发送邻居请求消息来确定邻居的链路层地址，或者验证邻居通过缓存的链路层地址仍然可达，邻居请求消息也可用于重复地址检测。

节点通过组播邻居请求消息完成地址解析，邻居请求消息要求目标节点返回它

的链路层地址。邻居请求消息组播到目标节点的请求节点组播地址，目标通过单播邻居通告消息返回链路层地址。发起者的邻居请求消息中包含链路层地址。

邻居请求消息也可以用来确定多个节点是否分配了相同的单播地址。重复地址检测的邻居请求消息在地址自动配置中规定。

（4）邻居通告

邻居请求消息的响应；节点也可以发送非请求邻居通告来指示链路层地址的变化。

邻居不可达检测可以检测邻居或邻居前向路径发生的故障，这样就要求确认发送给邻居的包到达了那个邻居且正在被 IP 层进行处理。邻居不可达检测使用两种方法进行确认：一种是上层协议提供“连接正在处理”的确认，即先前发送的数据认为是正确发送（如最近收到新的确认）；另一种是节点发送单播邻居请求消息，请求的邻居通告消息作为下一跳的可达性确认。为了减少不必要的网络流量，探测消息仅发送到邻居。

在路由器故障或链路层地址改变的链路和节点故障的情况下，邻居不可达检测是提高包传送能力的一部分，如由于 ARP 缓存无效，移动节点没有失去任何连接而离开非连接。不像 ARP，邻居发现检测半链路的故障，避免发送流量到失去双向连接的邻居。

路由器通告消息不包含优先权字段，不必处理稳定性不同的路由器。邻居不可达检测将检测失效的路由器，并切换到工作的路由器。

（5）重定向

路由器用于通知主机到达目的地的最佳下一跳。

重定向包含新第一跳的链路层地址，单独的地址解析不必接收重定向。

多个前缀可以和同一链路有关，在默认情况下，主机从路由通告中获得所有在连接（on-link）前缀。但路由器可以配置成忽略路由器通告中的某些或所有前缀，在这种情况下，主机认为目的地是非连接，并发送流量到路由器，然后路由器发布合适的重定向。

IPv6 重定向的接收认为下一跳是在连接。在 IPv4 中，根据链路的网络掩码指示下一跳不是在连接，主机忽略重定向。IPv6 重定向机制和共享介质的重定向机制类似。在非广播和共享媒介链路中，节点不可能知道在连接目的地的所有前缀。

除了处理上述一般问题之外，邻居发现也可以处理下列情况。

- 链路层地址改变：如果节点得知自己的链路层地址改变，就会组播邻居通告包到所有节点，迅速更新无效的缓存链路层地址。发送非请求通告消息仅能提高可靠性（如在不可靠时）。邻居不可达检测算法保证所有节点可以可靠地发现新地址，时延可能会比较长。

- 入口负载均衡：在接收来自相同链路上多个网络接口的数据包时需要负载均衡。这个节点在相同接口分配了多个链路层地址，如单个网络驱动程序可以把多个网络接口卡表示为具有多个链路层地址的逻辑接口。负载均衡允许路由器省略路由器通告包中的源链路层地址，强制邻居使用邻居请求消息了解路由器的链路层地址。请求消息发送者不同，返回的邻居通告消息包含不同的链路层地址。
- 任播地址：任播地址用于标识提供同样服务的一组节点，可以配置相同链路上的多个节点，能够识别相同的任播地址。通过节点接收对相同目标的多个邻居通告、邻居发现来处理任播。所有的任播地址的通告标记为 non-override 的通告，这样可以使用特定的规则来确定应该使用哪个通告。
- 代理通告：如果目标地址不能响应邻居请求，愿意代表该目标地址接收包的路由器会发布 non-override 的邻居通告。目前没有规定代理的使用，代理通告可以处理离开非连接（off-link）的移动节点，但不能作为通用的机制来处理节点。

使用链路本地地址唯一标识路由器（对于路由器通告和重定向消息），主机能在站点重编号且使用新的全球前缀时保持路由器联系。

邻居发现使用的跳数限制等于 255，可以防止非连接发送者故意发送邻居发现消息。在 IPv4 中发送者既发送重定向消息，也发送路由器通告消息。

## 3.4.2　ICMPv6 协议

ICMP 是为 IPv4 定义的，IPv6 使用时做了不少改动。IPv6 下一个头的值为 58 时表示为 ICMPv6 消息。ICMPv6 由 IPv6 节点使用，用于报告在分组处理过程中出现的错误，以及执行其他网络互连功能，如使用 ICMPv6“PING”进行故障诊断。ICMPv6 是 IPv6 的整体部分，是基础协议之一，由 IETF RFC 4443 规定，该 RFC 中规定的所有消息和行为对于每个 IPv6 节点来说都必须无条件执行。

在每个 ICMPv6 消息之前都有 IPv6 头和若干个 IPv6 扩展头。ICMPv6 头由其值为 58 的下一个头的值标识。

ICMPv6 消息的通用格式如图 3-23 所示。


图 3-23　ICMPv6 通用消息格式

各字段说明如下：

- 类型：指出消息类型。它的值决定其余的数据格式。

- 代码：依赖于消息类型。它用于生成消息粒度的附加层。
- 校验和：用于检测 ICMPv6 消息和 IPv6 首部部分中的数据错误。

ICMPv6 消息分为两类：出错消息和指示消息。出错消息由在它们的消息类型字段中的二进制值的高阶位取 0 标识。

# 3.5 IPv6 路由机制

IPv6 采用了与 IPv4 类似的路由机制。IPv6 路由系统包含两部分——内部路由与外部路由。

自治域（AS）允许描述一组路由器从内部路由到外部路由的转变。IP 数据包通常要穿过两个或多个 AS 的路由器才能到达目的地，AS 系统必须相互提供拓扑信息才能允许这种转发。内部网关协议用于在 AS 内部分发路由信息（即内部路由）；外部网关协议用于在 AS 间交换路由信息（即外部路由）。

## 3.5.1 内部网关协议

### 1．定义

内部网关协议（IGP）用于在特定 AS 内部路由器间分发路由信息。对特定 IGP 算法的实现相对独立，但必须实现下列功能：

- 应能迅速反映 AS 内部拓扑的改变；
- 提供一种机制使电路振荡时不引起连续的路由更新；
- 提供快速收敛成无环回（loop-free）路由；
- 使用最少的带宽；
- 提供等效路由以便负荷分担；
- 提供一种认证的路由更新方法。

IPv6 中目前规定了三种内部网关协议：RIPng、OSPFv3 及 IS-ISv6。

### 2．开放最短路径优先协议第三版——OSPFv3

基于最短路径优先（SPF）是一类基于链路状态算法的协议，它们基于 Dijistra 的最短路径算法。在基于 SPF 的系统中，每个路由器通过称为洪泛（flooding）算法的过程得到完整的拓扑数据库。洪泛过程确保信息可靠传输。每一个运行 SPF 算法的路由器在数据路上建立 IP 路由表。

在 IPv4 网络中，OSPF 协议的版本号为 2，也就是人们常说的 OSPFv2。为了支持 IPv6 网络，IETF 对 OSPFv2 协议进行了修改，形成了 OSPFv3。

IPv6 的 OSPF 协议保留了 IPv4 的大部分算法。从 IPv4 到 IPv6，基本的 OSPF 机制保持不变。IPv6 与 IPv4 都包含链路状态数据库，链路状态通告信息（LSA）包含在链路状态数据库中，并且相邻路由器中的这些信息要保持同步。初始数据库同步通过数据库交换过程来完成，这一过程包括交换数据库描述包、链路状态请求包、链路状态更新包。其后的数据库同步通过洪泛来维护，使用链路状态更新包和链路状态确认包来完成。在广播型和非广播多接入型（NBMA）网络中，IPv6 与 IPv4 都采用 OSPF 的 Hello 包发现与维护邻居关系，选举指派路由器和备份指派路由器。在其他方面，IPv6 与 IPv4 也保持一致，如决定哪个邻居关系变为相邻、域间路由的基本思想、引入 AS 外部 LSA 的外部信息及不同的路由计算。

IPv4 中的下面一些 OSPF 功能在 IPv6 中保持完全一致。

- IPv4 与 IPv6 都采用相同的包类型，即 Hello 包、数据库描述包、链路状态请求包、链路状态更新包、链路状态确认包。在某些情况下（如 Hello 包），包格式有些变化，但这些包的功能保持不变。
- 因为 OSPF 是直接运行在 IPv6 网络层之上的，IPv6 中的 OSPF 需要 IPv6 协议栈，但实现 OSPF 系统要求保持不变。
- 发现与维护邻居关系，以及邻接（adjacencies）关系的选择与建立保持不变。这包括在广播型和 NBMA 型网络中选举指派路由器和备份指派路由器。
- OSPF 支持的链路类型（或接口类型）保持不变，即点对点、广播、NBMA、点对多点及虚链路。
- 接口状态机，包括 OSPF 接口状态和事件的列表，指派路由器和备份指派路由器的选举算法均保持不变。
- 邻居状态机（包括 OSPF 邻居状态和事件的列表）均保持不变。
- 链路状态数据库的老化（Aging），以及通过未过期的老化过程在路由域中更新 LSA，均保持不变。

（1）OSPF 功能在 IPv6 中与 IPv4 中的不同之处

由于 IPv6 协议语义的变化，以及 IPv6 地址空间的增大，IPv6 的 OSPF 协议与 IPv4 的 OSPF 协议存在很多不同。

① 在链路上（不是在子网上）处理协议。

IPv6 使用术语“链路”，表示节点在链路层进行通信所经过的通信设备或介质。“接口”和链路相连，多个 IP 子网可以分配一个链路，不在同一个 IP 子网的两个节点可以在单个链路上直接通信。

因此基于 IPv6 的 OSPF 运行在每条链路上，基于 IPv4 的 OSPF 运行在每个 IP 子网上。在 IPv4 的 OSPF 规范中的术语“网络”和“子网”由“链路”取代，OSPF 接口与链路相连，而不是与 IP 子网相连。

② 删除了地址语义。

在基于 IPv6 的 OSPF 中，OSPF 协议包和主要的 LSA 类型删去了地址语义：

- 除了在链路状态更新包载有的 LSA 净荷外，OSPF 包中不出现 IPv6 地址；
- 路由器 LSA 和网络 LSA 不再包含网络地址，只简单地表示拓扑信息；
- OSPF 路由器 ID 和 LSA 链路状态 ID 保留为 IPv4 的 32 位大小，它们不再分配 IPv6 地址；
- 邻居路由器由路由器 ID 标识，在广播和 NBMA 网络上不再使用 IP 地址标识。

③ 增加了洪泛范围。

LSA 的洪泛范围体现在 LSA 的 LS 类型字段上，LSA 有三种洪泛范围。

- 链路本地范围。LSA 仅在本地链路洪泛，链路 LSA 使用这个范围。
- 域范围。LSA 仅在单个 OSPF 域内洪泛，路由器 LSA、网络 LSA、域间前缀 LSA、域间路由器 LSA、域内前缀 LSA 使用这个范围。
- 自治域范围。LSA 在路由域范围洪泛，AS 外部 LSA 使用这个范围。

④ 每条链路支持多个实例。

OSPF 支持在单条链路上运行多个 OSPF 协议实例的功能。例如，在几个运营者共享的 NAP 点上，运营者拥有共同的一个和多个物理网段（如链路），在这种情况下，运营者可以运行独立的 OSPF 路由域。

⑤ 链路本地地址的使用。

IPv6 链路本地地址用于单个链路上的邻居发现、自动配置等，IPv6 路由器不转发含有链路本地源地址的 IPv6 数据包。分配给链路本地单播地址的 IPv6 地址范围为 FF80::/10。

每个路由器在连接的物理段上分配了链路本地单播地址。除了虚链路的所有 OSPF 接口，与接口相关的链路本地地址可作为源地址来发送 OSPF 包。路由器可以了解到与链路连接的所有其他路由器的链路本地地址，并使用这些地址作为下一跳信息进行包转发。

在虚链路上，OSPF 协议包必须使用全球范围或本地站点的 IP 地址作为源地址。

链路本地地址出现在 OSPF 链路 LSA 中，但不允许出现在其他 LSA 类型里，并且链路本地地址不能在域间前缀 LSA、AS 外部 LSA 或域内前缀 LSA 中通告。

⑥ 验证的变化。

在 IPv6 的 OSPF 包头中删去了验证类型和验证字段，所有和验证相关的字段在 OSPF 域和接口结构中不再出现。

IPv6 的 OSPF 使用 IP 认证头和 IP 封装安全净荷，来提供完整性和机密性的安全保护。

⑦ 包格式的变化。

IPv6 的 OSPF 直接运行在 IPv6 上。OSPF 包头不包含地址语义，而是包含在不

同的 LSA 类型中，因此 IPv6 的 OSPF 与网络协议无关。

OSPF 包格式的变化如下。

- OSPF 版本号从 2 增加到 3。
- Hello 包和数据库描述包的可选字段扩展到 24 比特。
- OSPF 包头删去了验证和验证类型字段。
- Hello 包不包含地址语义，而是包含一个分配给发起路由器标识链路接口的接口 ID。如果路由器成为链路上的 DR，接口 ID 就是网络 LSA 的链路状态 ID。
- 为了在 SPF 计算时处理路由器 LSA，在选项字段中增加了两个选项比特：R 比特和 V6 比特。如果 R 比特置为 0，则 OSPF 发言者不转发穿越式流量，就可参与 OSPF 拓扑信息分布，如多穴主机需要参与路由协议的情况；如果 V6 比特置为 0，则 OSPF 发言者不转发 IPv6 的数据报就可参与 OSPF 拓扑信息分布；如果 R 比特置为 1，V6 比特置 0，则不转发 IPv6 数据包，但转发另一个协议的数据包。
- OSPF 包头包含一个“实例 ID”（instance ID），允许在一个单独的链路上运行多个 OSPF 协议实例。

⑧ LSA 格式的变化。

在 LSA 头和路由器 LSA、网络 LSA 中删去了所有地址语义，这两个 LSA 以网络协议无关的方式描述了路由域的拓扑。另外，还增加了用于分布 IPv6 地址信息的新 LSA，以及进行下一跳解析所需要的数据。

LSA 格式的具体变化如下。

- LSA 头删去了选项字段，而加入到路由器 LSA、网络 LSA、域间路由器 LSA 和链路 LSA 主体中，并扩展为 24 比特。
- LSA 类型字段扩展为 16 比特，前面 3 比特用于解码洪泛范围和处理未知的 LSA 类型。
- LSA 中的地址表示为[前缀，前缀长度]，而不是[地址，掩码]，默认路由的前缀长度为 0。
- 路由器和网络 LSA 没有地址信息，与网络协议无关。
- 路由器接口信息可通过多个路由器 LSA 扩散。当进行 SPF 计算时，接收者必须将给定路由器生成的所有路由器 LSA 连接起来。
- 链路 LSA 有本地链路洪泛范围，不会洪泛到链路以外。链路 LSA 有三个作用：提供路由器的链路本地地址，这个地址可以到达与链路相连的所有其他路由器；通知其他路由器和链路有关，这些路由器与 IPv6 前缀列表里的链路连接；允许路由器维护和网络 LSA 有关的选项字段的集合，其中网络 LSA 由链路生成。
- 第三类汇总 LSA 更名为“域内前缀 LSA”，第四类汇总 LSA 更名为“域

内路由器 LSA”。

- 域间前缀 LSA、域内路由器 LS 和 AS 外部 LSA 的链路状态 ID 仅用来标识单个的链路状态数据库，不包含地址语义。所有地址或路由器 ID 不再由链路状态 ID 表示，而是位于 LSA 的主体中。
- 网络 LSA 和链路 LSA 的链路状态 ID 是链路上发起路由器的接口 ID，因此网络 LSA 和链路 LSA 的大小不受限制。网络 LSA 必须列出连接链路的所有路由器，链路 LSA 必须列出链路上所有路由器的地址。
- 域内前缀 LSA 载有所有的 IPv6 前缀信息，IPv4 中这些信息包含在路由器 LSA 和网络 LSA 里。
- AS 外部 LSA 可选地址包含转发地址，可选地址包含外部路由标签。另外，AS 外部 LSA 可以参考其他 LSA，以及 OSPF 协议范围外的路由属性，如使用在连接 BGP 路径属性和外部路由的情况下。

⑨ 处理未知 LSA 类型。

在 IPv6 中，未知 LSA 类型可以看作具有本地链路洪泛范围，或者看作已知 LSA 类型进行存储和洪泛。而 IPv4 的 OSPF 只是简单地丢弃未知 LSA 类型。

⑩ 支持末梢域。

与 IPv4 的 OSPF 相同，设计末梢域的目的是减小域内路由器的链路数据库和路由表的大小，路由器用较少的资源可以处理较大的 OSPF 路由域。在 IPv6 中，末梢域仅能处理路由器 LSA、网络 LSA 和域内前缀 LSA，且允许未知类型的 LSA 作为已知类型的 LSA 来存储和洪泛，但需要控制这种 LSA 的处理，否则会导致末梢域链路状态数据库的膨胀而超过路由器的处理能力。

因此，对于末梢域建立了下列规则：如果 LSA 有域或本地链路洪泛范围且 LSA 的 U 比特设置为 0，那么未知类型的 LSA 可以在末梢域洪泛。

⑪ 使用路由器 ID 标识邻居。

在 IPv6 的 OSPF 中，给定链路上的邻居路由器由它们的 OSPF 路由器 ID 来标识。在 IPv4 的 OSPF 中，点到点网络和虚链路上的邻居由它们的路由器 ID 标识，广播、NBMA 和点到多点链路上的邻居由 IPv4 接口地址标识。

0.0.0.0 的路由器 ID 作为预留，不能使用。

⑫ 协议数据结构。

在 IPv4 和 IPv6 中，主要的 OSPF 数据结构都相同，如区域、接口、邻居、链路状态数据库和路由表。

基于 IPv6 的最高层数据结构保留了 IPv4 的大部分内容，一些变动如下：所有已知 LS 类型和 AS 洪泛范围的 LSA，不再属于某一特定区域或链路，而是归到最高层数据结构。AS 外部 LSA 是此规范中定义的唯一带有洪泛范围的 LSA。未知 LS 类型、U 比特置 1 的 LSA（尽管不能识别，但也要洪泛）及 AS 洪泛范围也要归到最高层数据结构。

IPv6 区域数据结构包含 IPv4 区域定义的所有单元，如区域 ID、区域地址范围列表、相关路由器接口、路由器 LSA 列表、网络 LSA 列表、汇总 LSA 列表、最短路径树、穿越能力、外部路由能力、末梢默认费用。另外，所有类型已知并带有区域洪泛范围的 LSA 也包含在 IPv6 区域数据结构中，通常包括以下 LSA 类型：路由器 LSA、网络 LSA、域间前缀 LSA、域间路由器 LSA 和域内前缀 LSAs。未知 LS 类型、U 比特置 1 的 LSA（尽管不能识别，但也要洪泛）和域范围也要归到区域数据结构。实现 MOSPF 的 IPv6 路由器还需把组成员 LSAs 加到区域数据结构中，第 7 类 LSAs 属于 NSSA 区域的数据结构。

在 IPv6 的 OSPF 中，接口连接路由器到链路上。IPv6 的接口结构对 IPv4 的接口结构进行了以下修改。

- 接口 ID：每个接口分配一个接口 ID，唯一标识路由器的接口，如一些实现可能采用 MIB-II 的 IfIndex 作为接口 ID。接口 ID 可能出现在以下包中，如从接口发出的 Hello 包，由路由器对相连链路发起的链路本地 LSA，由路由器 LSA 对相关区域发起的路由器 LSA。如果路由器选为指派路由器，接口 ID 也可作为网络 LSA 的链路状态 ID。
- 实例 ID：每个接口分配一个实例 ID。默认为 0，如果链路包含 OSPF 路由器的多个独立组（communities），就要为这些链路分配不同的值。例如，如果在一个以太网网段中有路由器的两个组，就需将它们分隔开。由于该路由器的所有以太网接口的实例 ID 分配为 0，所以第 1 组分配的实例 ID 为 0，路由器的其他以太网接口分配的实例 ID 为 1，这样 OSPF 的发送和接收过程将保持两组分隔。
- 带有链路本地范围的 LSA 列表：具有本地链路范围的所有 LSA，并在链路上发起/洪泛，都属于与此链路相连的接口结构。这包括链路的链路 LSA 集合。
- 带有未知 LS 类型的 LSA 列表：带有未知 LS 类型且 U 比特置 0 的所有 LSA（如果不能识别，就做链路本地洪泛范围处理 LSA）都保存在接收此 LSA 的接口数据结构里。
- IP 接口地址：对于 IPv6，由接口发出的源 OSPF 包的 IPv6 地址几乎总是链路本地地址。唯一的例外是对虚链路，必须用路由器自己的全局 IPv6 地址作为 IP 接口地址。
- 链路前缀列表：可以为相连链路配置的 IPv6 前缀列表，然后路由器在链路 LSA 中通告，因此就能通过指派路由器在域间前缀 LSA 中通告。

在 IPv6 的 OSPF 中，每个路由器接口都有一个度量，表示从此接口发出包的费用。另外，IPv6 的 OSPF 依靠 IP 验证头和 IP 封装安全净荷来保证路由交换的完整性和认证/机密性。因此，AuType 和认证的密钥与 IPv6 的 OSPF 接口无关。

接口状态、事件及状态机与 IPv4 保持一致。指派路由器和备份指派路由器的选

举算法也与 IPv4 中的选举保持一致。

在 IPv6 和 IPv4 中，邻居结构完成相同的功能，即如果两个路由器有必要建立邻接，该结构就收集所有建立邻接需要的信息。IPv6 的邻居结构和 IPv4 邻居结构的不同点在于以下几方面。

- 邻居的接口 ID：邻居在 Hello 包中通告的接口 ID 必须记录在邻居结构中。当路由器向邻居通告点对点链路，或在邻居已成为指派路由器的网络中通告一条链路时，必须在路由器的路由器 LSA 中包括邻居的接口 ID。
- 邻居 IP 地址：除了在虚链路上，邻居的 IP 地址就是 IPv6 的链路本地地址。
- 邻居的指派路由器：邻居的指派路由器的选取以路由器 ID 来编码，而不是 IP 地址。
- 邻居的备份指派路由器：邻居的备份指派路由器的选取以路由器 ID 来编码，而不是 IP 地址。

邻居状态、事件及邻居状态机与 IPv4 保持不变，关于建立哪种邻接也与 IPv4 保持不变。

OSPFv3 协议的具体实现可以参考 IETF RFC 5340。

### 3．IPv6 中间系统到中间系统协议——IS-ISv6

IS-ISv6 是基于链路状态（SPF）路由算法，拥有所有该类协议的优点。

ISO/IEC 10589 规定的 IS-IS 协议是一个可扩展的路由协议，可支持 IPv4、IPv6 及 OSI 路由信息的传送。IETF RFC 1195 规定了 IPv4 路由信息的传送方式（IS-IS），IETF RFC 5308 规定了 IPv6 路由信息的传送方式（IS-ISv6）。

IS-ISv6 协议是对 IS-IS 协议的扩充，其基本的消息格式及路由信息传送处理规程与 IS-IS 相同，主要的区别在于消息中增加了传送 IPv6 路由和地址信息所需要的属性，扩展了两种新的 TLV 类型，即可达性 TLV 和接口地址 TLV，利用这两种 TLV 可在路由域中发布 IPv6 路由信息。

#### （1）IPv6 可达性 TLV

IPv6 可达性 TLV 的 TLV 类型值是 236（0xEC）。

IETF RFC 1195 中定义了两种可达性 TLV，即“IP 内部可达性信息”和“IP 外部可达性信息”，在 IS-ISv6 中用“IPv6 可达性”TLV 和一个“外部”比特提供了等效的 IPv6 路由功能。

“IPv6 可达性”TLV 中包含路由前缀和权值信息；包含 U 比特，用于指明该前缀是否是从更高等级上向下发布的；包含 X 比特，用于指明该前缀是否是另一个路由协议发布的；此外，还可以包含“子 TLV”（可选项），以便将来进行扩展。“IPv6 可达性”TLV 通过对这些数据进行规定来描述网络的可达性，数据的格式如图 3-24 所示。

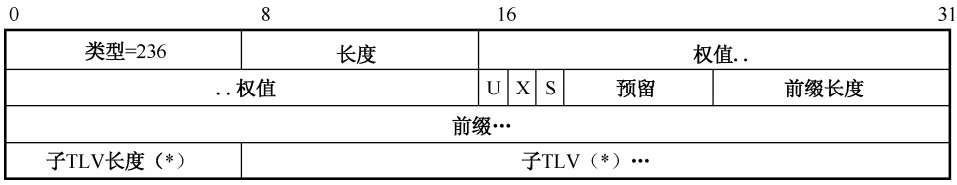



图 3-24　IPv6 可达性 TLV 的格式

图中，*表示可选项，U 表示上/下比特，X 表示外部比特，S 表示子 TLV 比特。

IPv6 可达性 TLV 可以在 LSP 中出现任意多次（也可以不出现）。当一个前缀是第一次注入 IS-IS 中时，上/下比特被置为“0”。如果前缀是从一个较高等级重发布到一个较低等级上（如从等级 2 到等级 1），则该比特别置为“1”，以表明该前缀是按从高向低等级发布的。如果前缀是从等级相同的一个区域重发布到另一个区域，则上/下比特被置为“1”。

如果前缀是从另一个路由协议发布到 IS-IS 中的，则外部比特被置为“1”。从 IS-IS 向其他协议发布前缀时这一信息是有用的。

如果“子 TLV”比特被置为“0”，则不出现“子 TLV”；否则，如果该比特被置为“1”，则前缀后边的一个字节就是描述“子 TLV”长度的字节，且格式中包含“子 TLV”部分。前缀被“打包”到数据结构中，这是指只有前缀所需要的若干字节出现在数据结构中。字节数目可以根据前缀长度计算得到，具体如下：

前缀字节数＝取整（（前缀长度+7）/8）

如果发布的前缀具有大于 MAX_V6_PATH_METRIC（0xFE000000）的权值，则在进行通常的 SPF 计算时禁止考虑该前缀。这种处理方式下，为了建立通常的 IPv6 路由表以外的原因而发布一个前缀是被允许的。

如果有子 TLV，则其格式与普通的 TLV 相同，见图 3-25。

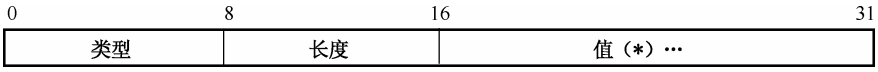



图 3-25　IPv6 可达性 TLV 的子 TLV 格式

图中，*表示可选项，长度字段指明值字段有多少字节，长度字段值可为零。

（2）IPv6 接口地址 TLV

IPv6 接口地址 TLV 的 TLV 类型值是 232（0xE8）。

这个 TLV 直接映射到 IETF RFC 1195 规定的“IP 接口地址”TLV 中。为此需要对内容进行调整，用序号为 0～15 的 16 字节的 IPv6 接口地址取代序号为 0～63 的 4 字节的 IPv4 接口地址，数据的格式如图 3-26 所示。

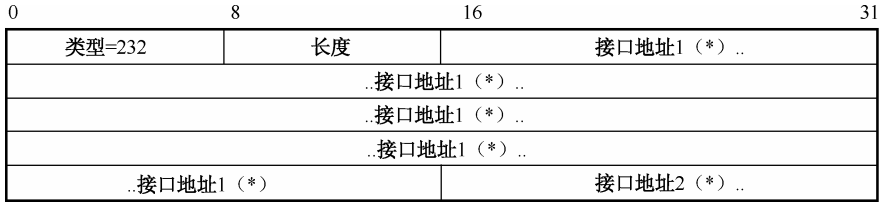



图 3-26　IPv6 接口地址 TLV

图中，*表示可选项。

根据 TLV 是否被发布，在此对 TLV 的句法做进一步的限制。对于 Hello PDU，“接口地址”TLV 必须只包含分配给发送 Hello 消息的接口的链路本地 IPv6 地址。对于 LSP，“接口地址”TLV 中必须只包含分配给 IS 的非链路本地 IPv6 地址。

（3）IPv6 NLPID

IPv6 NLPID 的值是 142（0x8E）。

参照 IPv4 及 IETF RFC 1195 的规定，如果 IS 用 IS-IS 协议支持 IPv6 路由，则必须将 IPv6 NLPID 添加到“NLPID”TLV 中发布。

如果有两条路径对应于一个给定的前缀，则对路径进行优选时必须考虑根据上/下比特进行调整。新的优选次序如下：

① 等级 1 上前缀；

② 等级 2 上前缀；

③ 等级 2 下前缀；

④ 等级 1 下前缀。

如果多条路径具有同样的最好优选等级，则要根据权值进行选择。如果路由器支持相等开销多径路由，则多条路径应被看作相等开销的多径路由，否则路由器可以选择多条路径中的任意一条。

### 4．下一代路由信息协议——RIPng

路由信息协议 RIP 是 IETF 最早开发和应用的基于 IPv6 的动态 IP 路由协议之一，目前的版本是 RIPv1 和 RIPv2。1997 年，随着 IETF 制定 IPv6 标准的进展，为了解决 RIP 协议与 IPv6 的兼容性问题，IETF 对 RIP 协议进行了改进，制定了基于 IPv6 的下一代路由信息协议 RIPng（RIP next generation）标准，定义在 IETF RFC 2080 中。RIPng 应用极其广泛，是自治域内路由协议的事实标准之一。

RIPng 的目标并不是创造一个全新的协议，而是对 RIP 进行必要的改造以使其适应 IPv6 下的选路要求，因此 RIPng 的基本工作原理同 RIP 是一样的，这主要体现在以下方面。

- RIPng 路由机制基于距离矢量协议。
- RIPng 通过 UDP 报文交换路由信息，使用的 UDP 端口是 521（RIP 使用 520）。

- RIPng 每 30s 发送发送一次路由更新包，如果 180s 没有收到邻居的更新信息，则将其置为不可达；如果再过 120s 还未收到路由更新，则将其从路由中删除。
- 为了避免环路，RIPng 也使用了水平分割和毒性反转技术。
- 相对于 RIPv1 和 RIPv2，RIPng 主要的变化在地址和报文格式方面。
- 地址空间。RIPv1、RIPv2 是基于 IPv4 的，地址空间为 32 比特，而 RIPng 是基于 IPv6 的，使用的所有地址均为 128 比特。
- 子网掩码和前缀长度。RIPv1 被设计成用于无子网的网络，因此没有子网掩码的概念，这就决定了 RIPv1 不能用于传播变长的子网地址或用于 CIDR 的无类型地址。RIPv2 增加了对子网选路的支持，因此使用子网掩码区分网络路由和子网路由。IPv6 的地址前缀有明确的含义，因此 RIPng 中不再有子网掩码的概念，取而代之的是前缀长度。同样也是由于使用了 IPv6 地址，RIPng 中也没有必要再区分网络路由、子网路由和主机路由。
- 协议的使用范围。RIPv1、RIPv2 的使用范围被设计成不只局限于 TCP/IP 协议族，还能适应其他网络协议族的规定，因此报文的路由表项中包含有网络协议族字段，但实际的实现程序很少被用于其他非 IP 的网络，因此 RIPng 中去掉了对这一功能的支持。
- 对下一跳的表示。RIPv1 中没有下一跳的信息，接收端路由器把报文的源 IP 地址作为到目的网络路由的下一跳。RIPv2 中明确包含了下一跳信息，便于选择最优路由和防止出现选路环路及慢收敛。与 RIPv2 不同，为防止 RTE 过长，同时也是为了提高路由信息的传输效率，RIPng 中的下一跳字段是作为一个单独的 RTE 存在的。
- 报文长度。RIPv1、RIPv2 中对报文的长度均有限制，规定每个报文最多只能携带 25 个 RTE。而 RIPng 对报文长度、RTE 的数目都不作规定，报文的长度是由介质的 MTU 决定的。RIPng 对报文长度的处理提高了网络对路由信息的传输效率。
- RIPng 使用 FF02::9 这个地址进行组播更新。
- 由于 RIPng 运行于 IPv6 协议之上，因此 RIPng 依赖于 IPv6 协议中规定的 IP 认证扩展头及 IP 封装安全载荷扩展头来确保协议完整性及路由信息交换过程中的加密认证，自身不再提供身份验证机制。

RIPng 协议的具体实现可以参考 IETF RFC 2080。

## 3.5.2　外部网关协议

### 1．概述

外部网关协议在自治系统间使用，为特定自治系统内一组网络与相邻自治系统

交换可达性信息。

当前，IPv4 网络上主要应用的域间路由协议是 BGP4 协议。BGP 协议用于在 BGP 运行者之间交换网络可达性信息。网络信息包含流量到达某个网络所必须经过的完整 AS 列表。BGP 协议最初被设计时只能广播 IPv4 的域间路由信息，协议中规定的以下三种属性是明确与 IPv4 协议相关的。

- NEXT_HOP 属性（使用 IPv4 地址表示）；
- AGGREGATOR 属性（存储 IPv4 地址）；
- NLRI 属性（利用 IPv4 的地址前缀表示）。

为了使 BGP4 能够支持多种网络层协议，如 IPv6、IPX 等，IETF 制定了 IETF RFC 4760，其中定义了 BGP4 协议的扩展机制，该机制可使 BGP4 协议携带多种网络层协议（如 IPv6、IPX 等网络层协议）的路由信息。

该机制中，首先假定任何一个 BGP 发言者（包括支持多协议扩展功能的发言者）都具有一个 IPv4 地址，因此，欲使 BGP4 协议能够支持多种网络层协议进行路由选择，必须在 BGP4 协议中增加如下两个功能。

- BGP4 新增的信息必须将某一特定网络层协议与下一跳信息相关联，即下一跳地址用指定的网络层协议地址表示。
- 具备将某一特定网络层协议与 NLRI 相关联的能力，需要使用地址族来区别不同的网络层协议。

当且仅当 BGP4 协议需要发布可到达目的地的路由消息时，消息中所包含的 NEXT_HOP 属性必须提供下一跳地址信息。当 BGP4 协议发布从服务器上撤销某些路由的不可到达的目的地路由信息时，NEXT_HOP 属性无须一定提供下一跳地址信息。因此，应将 BGP4 协议中的路由消息中所包含的可到达目的地信息与下一跳地址信息组合起来一起发布，并且可到达目的地的路由消息发布应该从不可到达目的地的路由消息发布中分离出来。

IETF RFC 4760 所规定的多协议扩展具有向后兼容性，如一台支持多协议扩展的路由器能够与一台不支持扩展的路由器相兼容。

另外，基于上述的多协议扩展机制，IETF 还制定了 IETF RFC 2545，规定了多协议扩展对 IPv6 协议的支持，从而实现了 BGP 协议在 IPv6 网络中的应用。

为了以示区别，通常把应用于 IPv6 网络的 BGP 协议称为 BGP+协议。

### 2．BGP4 多协议扩展

BGP4 多协议扩展主要扩展了两个新的路径属性：MP_REACH_NLRI 属性（多协议可到达 NLRI）和 MP_UNREACH_NLRI 属性（多协议不可到达 NLRI），如表 3-2 所示。通过这两个属性，BGP4 路由协议可以发布多种网络层协议（如 IPv6、IPX 等）的路由选择信息。

表 3-2　BGP4 多协议扩展新增路径属性列表

| 属　性　名 | 类　型　码 | 用　　途 |
|---|---|---|
| MP_REACH_NLRI | 14 | 用于承载可到达目的地集，以及用作这些目的地转发 |
| MP_UNREACH_NLRI | 15 | 用来承载不可到达目的地集合 |

这两个属性都是可选的属性和非传送属性。当不能支持多协议能力的 BGP 发言者接收到包含这两个属性的 BGP 消息时，应忽略这些属性中所包含的信息，并且不应将这些信息传送给其他 BGP 对等体。这种多协议扩展方式可以提供后向兼容性，即支持多协议扩展的路由器可以与不支持多协议扩展的路由器进行互通操作。

（1）MP_REACH_NLRI 属性

MP_REACH_NLRI 属性可用于如下目的。

- 向 BGP 对等体发布一条有效的路由；
- 允许路由器发布其网络层地址，其中网络层地址位于 MP_NLRI 属性的网络层可到达信息字段中，该地址用来作为目的地的下一跳地址。

MP_REACH_NLRI 属性的编码格式如图 3-27 所示。

| 地址族标识符（AFI）（2字节） |
|---|
| 子序列地址族标识符（SAFI）（1字节） |
| 下一跳网络地址长度（1字节） |
| 下一跳网络地址（可变长度） |
| 预留（1字节） |
| 网络层可到达信息（NLRI）（可变长度） |

图 3-27　MP_REACH_NLRI 属性的编码格式

各字段说明如下。

① 地址族标识符（AFI）：该字段长度为 2 字节，它与 SAFI 字段结合起来标识下一跳字段承载的地址所属的网络层协议的集合、下一跳地址的编码方式及 NLRI 字段的语义。如果下一跳允许来自多个网络层协议，则下一跳的编码必须提供确定其网络层协议的方式。

② 子序列地址族标识符（SAFI）：该字段长度为 1 字节，它与 AFI 字段结合起来标识下一跳字段承载的地址所属的网络层协议的集合、下一跳地址的编码方式及 NLRI 字段的语义。如果下一跳允许来自多个网络层协议，则下一跳的编码必须提供确定其网络层协议的方式。

③ 下一跳网络地址长度：该字段长度为 1 字节，其数值表示“下一跳网络地址”字段的长度，长度以字节为单位进行度量。

④ 下一跳网络地址：该字段长度可变，表示路径中到达目的地的下一个路由器的网络地址。属性中携带的网络层协议与下一跳网络地址的表示方法为<AFI，SAFI>。

⑤ 预留：该字段长度为 1 字节，必须设置为 0，接收方应忽略该字段。

（2）网络层可到达信息（NLRI）

该字段长度可变，用于承载这个属性发布的有效路由中所列出的 NLRI。NLRI 的语义通过属性中携带的<AFI，SAFI>组合来标识。

在 MP_REACH_NLRI 路径属性中承载的下一跳地址信息指定了路由器所使用的网络层地址，该路由器应该作为 UPDATE 消息中所包含 MP_NLRI 属性中所列出的目的地的下一跳。

下一跳地址信息的规则与 BGP4 协议中 NEXT_HOP 属性携带的信息的规则相同。

不管是在 EBGP 中还是在 IBGP 消息流程中，如果 UPDATE 消息承载了 MP_REACH_NLRI 属性，则该消息必须同时承载 ORIGIN 属性和 AS_PATH 属性。并且，在 IBGP 消息流程中，UPDATE 消息还必须承载 LOCAL_PREF 属性。

如果除了在 MP_REACH_NLRI 属性中承载有 NLRI 信息之外，UPDATE 消息中未承载其他 NLRI 信息，则 UPDATE 消息不应承载下一跳地址 NEXT_HOP 属性。如果 BGP 发言者接收到此类消息中包含 NEXT_HOP 属性，则 BGP 发言者应忽略消息中 NEXT_HOP 属性。

一个 UPDATE 消息不应在下面的字段中包含多于一个的相同的地址前缀（也就是相同的<AFI，SAFI>组合）：WTHEDRAWN ROUTES 字段、网络可达性信息字段、MP_REACH_NLRI 字段及 MP_UNREACH_NLRI 字段。

（3）MP_UNREACH_NLRI 属性

该属性能够用于从路由器中撤销若干不可到达路由，编码格式如图 3-28 所示。

| 地址族标识符（AFI）（2字节） |
| --- |
| 子序列地址族标识符（SAFI）（1字节） |
| 撤销的路由（可变长度） |

图 3-28　MP_UNREACH_NLRI 属性编码格式

各字段说明如下。

① 地址族标识符（AFI）：该字段长度为 2 字节，它与 SAFI 字段结合起来标识下一跳字段承载的地址所属的网络层协议的集合、下一跳地址的编码方式及 NLRI 字段的语义。如果下一跳允许来自多个网络层协议，则下一跳的编码必须提供确定其网络层协议的方式。

② 子序列地址族标识符（SAFI）：该字段长度为 1 字节，它与 AFI 字段结合起

来标识下一跳字段承载的地址所属的网络层协议的集合、下一跳地址的编码方式及NLRI 字段的语义。如果下一跳允许来自多个网络层协议，则下一跳的编码必须提供确定其网络层协议的方式。

③ 撤销的路由（Withdrawn Routes）。该字段长度可变，用于承载从服务中撤销的路由所列出的 NLRI。NLRI 的语义通过属性中携带的<AFI，SAFI>组合来标识。

如果 UPDATE 消息包含 MP_UNREACH_NLRI 属性，则该消息不需要承载任何其他路径属性。

（4）NLRI 编码

网络层可到达信息（NLRI）字段编码由一个或多个两维数组组成，两维数组格式为{长度，前缀}，字段编码方式如图 3-29 所示。

| 长度（1字节） |
| --- |
| 前缀（可变长度） |

图 3-29　NLRI 字段编码

各字段说明如下。

① 长度（Length）：该字段用于指示地址前缀字段的长度，以比特为单位进行度量。当其数值等于 0 时，表明地址前缀将匹配地址族标识符字段所指示的具有相同地址前缀的所有地址。

② 前缀（Prefix）：前缀字段包含一个地址前缀，在地址前缀的后面有足够多的填充比特，这些填充比特使该字段长度为字节的整数倍。需要指出的是，填充比特的数值是不相关的。

（5）子序列地址族标识符（SAFI）

MP_REACH_NLRI 属性和 MP_UNREACH_NLRI 属性中所包含的子序列地址族标识符（SAFI）字段定义的数值和含义分别如下：

- 网络层可到达信息用于单播转发；
- 网络层可到达信息用于组播转发。

（6）差错处理

如果一个 BGP 发言者接收到从邻居发来的一条包含 MP_REACH_NLRI 属性或 MP_UNREACH_NLRI 属性的 UPDATE 消息，并且接收方确定消息所包含的属性不正确，则消息接收方必须撤销所有那些从相同的邻居那里接收来的，并且具有与不正确的 MP_REACH_NLRI 或 MP_UNREACH_NLRI 属性中所承载的相同的 AFI/SAFI 的 BGP 路由。在接收到此错误 UPDATE 消息的 BGP 会话期间，BGP 发言者应该忽略所有此会话期间后续接收到的具有相同 AFI/SAFI 的路由。

除此之外，BGP 发言者可以中断接收到这种不正确 UPDATE 消息的 BGP 会话。会话中断应该使用 NOTIFICATION 消息，并且消息错误码为 Update Message Error，错误子码为 Optional Attribute Error。

（7）BGP 能力通告

使用多协议扩展的 BGP 发言者应该使用能力通告程序来确定是否能够与一个特定的对等体来进行多协议扩展 BGP 的能力交互。

BGP 可选能力参数字段中，能力代码字段设置为 1，用于指示支持多协议扩展能力，能力长度字段设置为 4，能力字段编码如图 3-30 所示。

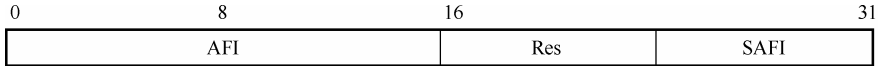



图 3-30　能力字段编码

该字段中各参数的含义和用途如下。

- AFI（地址族标识符），长度为 16 比特，编码方式同前所述。
- Res（预留字段），长度为 8 比特，消息发送方应将该字段设置为 0，消息接收方应忽略该字段。
- SAFI（子序列地址族标识符），长度为 8 比特，编码方式同前所述。

支持多个<AFI，SAFI>数组的 BGP 发言者应将它们作为可选能力参数的多个能力。

为了在一对指定的 BGP 发言者之间双向交换<AFI，SAFI>所指定的路由信息，每一个 BGP 发言者必须通过能力通告机制，将能支持<AFI，SAFI>所指定的路由的能力发布给对等体。

### 3．BGP4 多协议扩展对 IPv6 的支持

IETF RFC 2545 规定了利用 BGP4 多协议扩展定义的 MP_REACH_NLRI 和 MP_UNREACH_NLRI BGP 属性来传送 IPv6 路由信息的机制。

（1）基本要求

BGP4 协议和一般的距离向量路由协议一样，通常是独立于协议所用的特定地址族的。IPv6 协议属于 BGP4 协议所支持一种协议。

IPv6 和 IPv4 协议在路由信息方面最主要的不同是 IPv6 引入了区域化的单播地址，并且定义了必须使用特定地址范围的特定情况。

（2）IPv6 地址范围

IPv6 目前定义了两种单播地址范围：全局地址和链路本地地址。IPv6 的规范进

一步定义：只有链路本地地址可用于产生 ICMP 重定向消息（ND）；在一些路由协议中作为下一跳的地址（如 RIP）。这些限制暗示了一个 IPv6 路由器对于所有直连路由（即那些给出的路由器和下一跳路由器的子网前缀相同的路由）必须有一个链路本地下一跳地址。但是，根据 BGP4 协议规范中给出的下一跳属性的规则，链路本地地址并不太适合用作 BGP4 中下一跳的属性。

由于以上原因，当 BGP4 用于传送 IPv6 可达信息，在宣布下一跳属性时，某些时候需要同时包括一个全局地址和一个链路本地地址。

（3）构造下一跳域

BGP 发言者应将下一跳的全局 IPv6 地址在下一跳域的网络地址中通告给其对等体，下一跳的 IPv6 链路本地地址可能跟在其后。

当只有一个全局地址时，在 MP_REACH_NLRI 属性中下一跳网络地址域的长度值应该设置为 16，而如果一个链路本地地址也包含在下一跳域中时，此长度值应设置为 32。

只有在 BGP 发言者、下一跳域的网络地址中的 IPv6 全局地址标识的实体及此路由要发布给的对等体共享相同的子网时，链路本地地址才包括在下一跳域中。其他情况下，BGP 发言者在网络地址域通告给其对等体的只是下一跳的 IPv6 全局地址（下一跳域的网络地址长度值是 16）。

因此，BGP 发言者通告一条路由给内部对等体时可以通过去掉下一跳的链路本地 IPv6 地址来修改下一跳的网络地址。

（4）传输

BGP4 消息交互发生在 TCP 连接之上，而 TCP 连接基于 IPv6 和 IPv4 都可以建立。BGP4 自身独立于所使用的传输协议，只是用传输协议从建立对等会话的地址中获得隐含的配置信息。此信息（对等体的网络地址）在路由分发过程中要考虑进去。所以，用基于 IPv4 的 TCP 连接来传送 IPv6 可达信息时，要求有额外明确的对等体的网络地址配置信息。

以上提到的信息有别于用在 BGP4 解结过程中的 BGP 身份标识。BGP 身份标识是包含在 OPEN 消息里的一个 32 位无符号整数，在对等实体间建立会话时互相交换。这个 BGP 身份标识是整个系统适用的值，在启动时被确定，在网络中必须是唯一的；在给定时刻，无论一个特定 BGP4 实例被配置成传送何种网络层协议，此 BGP 身份标识都要从 IPv4 地址中获取。

用基于 IPv6 的 TCP 传输协议传送 IPv6 可达信息也有其优点，如可以在对等实体间提供 IPv6 可达的明确的确认。

# 3.6 IPv6 网络过渡技术

在 IETF 的研究中，提出了多种网络迁移技术和方法，归结起来可以分为如下三种策略：双栈策略、隧道策略和翻译策略。这些策略在实际组网应用中很少单独使用，通常多种技术相互配合，共同完成综合组网。

## 3.6.1 双栈策略

双栈策略是指在网元中同时具有 IPv4 和 IPv6 两个协议栈，这样，它既可以接收、处理、收发 IPv4 的分组，也可以接收、处理、收发 IPv6 的分组。对于主机（终端）来讲，“双栈”是指其可以根据需要来对业务产生的数据进行 IPv4 封装或 IPv6 封装；对于路由器来讲，“双栈”是指在一个路由器设备中维护 IPv6 和 IPv4 两套路由协议栈，使得路由器既能与 IPv4 主机通信也能与 IPv6 主机通信，分别支持独立的 IPv6 和 IPv4 路由协议，IPv4 和 IPv6 路由信息按照各自的路由协议进行计算，维护不同的路由表。IPv6 数据报按照 IPv6 路由协议得到的路由表转发，IPv4 数据报按照 IPv4 路由协议得到的路由表转发。双协议栈结构如图 3-31 所示。

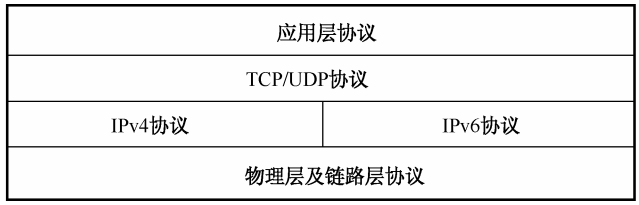



图 3-31 双协议栈结构

### 1. 应用方式

在支持 IPv4/IPv6 双栈的网络中，需要一个路由器维护两套协议规范，实际上相当于一台路由器硬件平台模拟了两个路由器，从而在一个物理 IP 网络中形成两个逻辑网络，一个是 IPv4 网络，另一个是 IPv6 网络。这两个逻辑网络同时能够覆盖整个物理网络。由于需要通信的网元均支持两种协议，也就是说这个网元同时属于两个 IP 逻辑网络，因此网元之间可以通过协商或按照域名解析结果来选择通信协议。从而实现网络对 IPv6 协议的支持。

上面所描述的是一种应用双栈策略组网的理想情况，而实际应用时可以灵活处理，如可以只对城域核心网和骨干网应用双栈策略，而边缘网络保持不变；也可在边缘网络采用双栈策略，而城域核心网和骨干网保持原有的 IPv4 网络不变。

对于前者，组网时对用户要求比较低，用户可以自己选择所采用的通信协议，但是核心网和骨干网路由器的升级更新工作较为繁重。这种方式下会遇到另外一个重要的问题：IPv4 的终端不能与 IPv6 终端进行通信，如果需要通信则需要采用地址/协议转换方法。

对于后者，用户终端的操作系统需要升级以支持双协议栈，而城域核心网和骨干网则可以继续采用原有的 IPv4 协议，保持网络结构和处理逻辑的简单性，从而使得网络相对稳定、可靠；但是这也会带来另外两个问题。

首先，由于用户终端数量较大，也是消耗 IP 地址的主要网元类型，由于其采用双协议栈，则其可能同时拥有 IPv4 地址和 IPv6 地址，因此 IPv4 地址并没有像预想的那样得到大规模的节省。当然，针对这种情况也可以继续采用原来 IPv4 网络中就已经采用的“临时地址”方式来在一定程度上减少公有 IP 地址的需求量，但是并没有从本质上解决 IPv4 地址不足的问题，也没有实现在网络中引入 IPv6 地址，以获得较大地址空间的目的。

其次，这种组网方式会出现 IPv6 终端（或子网）通过 IPv4 进行通信的需求，目前解决这个问题的方法有两个：一个是采用隧道技术；另一个是采用两次的地址/协议翻译。采用隧道技术时，IPv4 网络作为 IPv6 数据流的传输网络，这时有很多种具体的隧道技术存在，如手工配置隧道、6to4 隧道、6over4 隧道、GRE 隧道等，这些技术将在后面的章节中详细讨论。在这种情况下，采用地址/协议翻译技术效率低下，需要进行 IPv6 到 IPv4、IPv4 到 IPv6 的两层协议转换，因此通常不会在工程实践中采用。

### 2. 应用特点

总体来讲，上述双栈策略的优点是概念清晰、易于理解、网络规划相对简单，同时在 IPv6 逻辑网络中可以充分发挥 IPv6 协议的所有优点（如安全性、路由约束、流的支持等方面）。

但是双栈策略也存在如下缺点：对网元设备的要求较高，要求其不但支持 IPv4 路由协议，而且支持 IPv6 路由协议，这就要求其维护大量的协议和数据。一种改进的方案是采用一种兼容 IPv6 和 IPv4 双协议规范的路由协议，但到目前为止还没有这样的协议规范出现。另外，网络升级改造将牵涉网络中的所有网元设备，投资大、建设周期比较长。

### 3. 应用范围

正如前面所分析的那样，双栈策略可以灵活地应用在网络的各个侧面，如主机（终端）、网络边缘（接入和汇聚层）、核心骨干层等。但是通常双栈策略在这些网络层次应用时，需要注意以下几个方面的问题。

首先，如果单纯地采用双栈策略（不配合采用隧道和翻译机制）来升级网络，则要求在全网范围内全部统一，这需要网络的整体割接，否则会出现网络中的某些部分为路由不可达的情况。而网络的整体割接实际上不现实，因此在网络中某个部分采用双栈策略时，通常需要其他策略的配合（如隧道策略和翻译策略），来共同实现 IPv4/v6 综合组网。

其次，采用双栈策略的网元具有两个协议栈，但是不一定同时拥有 IPv4 地址和 IPv6 地址，由于 IPv6 地址空间充足，可以做到每个网元拥有一个或多个 IPv6 地址，而 IPv4 地址则可以根据实际需求来临时分配。

目前双栈策略在主机（终端）中应用较多，但是其很少单独使用。例如在 BIS、BIA 技术中都要求主机（终端）支持双协议栈。

对于网络边缘部分来讲，可以应用的基于双栈策略的具体技术主要有 DSTM 技术。

对于城域核心层和骨干网来讲，目前双栈策略应用较少，基本上采用原有的 IPv4 网络（有时结合采用 MPLS 技术）作为基础网络，通过在网络边缘采用隧道策略为 IPv4 和 IPv6 数据提供传输通道。

#### 4. 典型技术：DSTM

DSTM（Dual Stack Transition Mechanism）目前在 IETF 还属于草案阶段（2003 年依然没有成为 RFC）。使用 DSTM 机制的节点必须是双栈节点，同时在应用中还需要结合隧道技术。

（1）应用场景

DSTM 技术主要解决 IPv6 网络中的双栈主机（平时只有 IPv6 地址而无 IPv4 地址）如何与外部 IPv4 网络中的网元（只拥有 IPv4 地址）进行通信的问题。DSTM 技术只能应用在内部网络（企业网或驻地网），它不是一个可以应用在骨干网和核心网中的技术。

（2）基本原理

DSTM 的出发点是为纯 IPv6 网络（企业网或驻地网）中的双栈节点（只拥有 IPv6 地址）提供一个获得 IPv4 地址的方式（为双栈节点分配临时 IPv4 地址的方式），从而使之能够利用 IPv4-over-IPv6 隧道机制，实现通过纯 IPv6 网络与外部纯 IPv4 网络中的纯 IPv4 节点或 IPv4 应用程序进行通信的目的，具体如图 3-32 所示。

（3）功能构件

DSTM 的体系结构中包括：一个 DSTM（地址）服务器，一个网关，或者是隧道端点和若干 DSTM 节点。

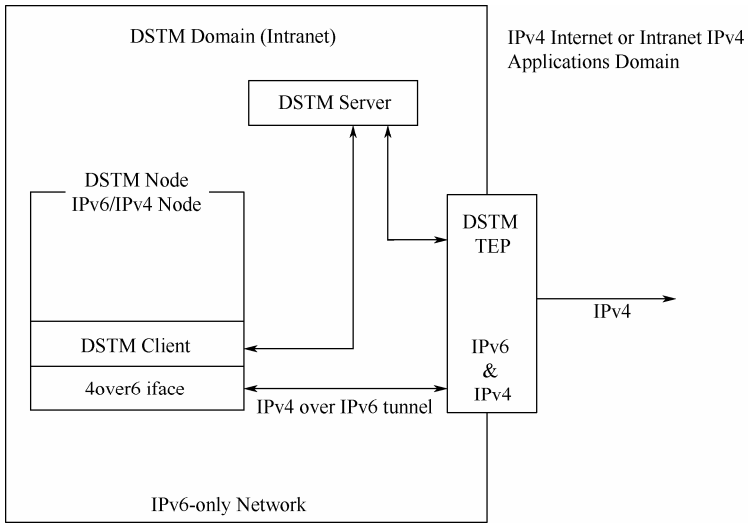



图 3-32　DSTM 的基本原理

DSTM 服务器维护一个 IPv4 地址池，并负责根据 DSTM 节点的请求为其分配 IPv4 地址（包括多种方式，如有状态的 DHCPv6 和无状态的地址自动配置方法等），DSTM 服务器只需要保证 DSTM 节点所获得的 IPv4 地址在一定的时间内是唯一的、有效的。

DSTM 节点在获得了 IPv4 地址以后，把由业务产生的 IPv4 包封装在 IPv6 数据包中，建立 4over6 隧道到隧道端点 TEP，利用 IPv4 over IPv6 技术把 IPv4 包发送到网关（TEP）。相反，可以从 TEP 处获得封装有 IPv4 数据的 IPv6 包，并完成 IPv6 包的解封装。

网关或隧道终点 TEP 是纯 IPv6 域和外部的 IPv4 网络的边界路由器，它一方面负责与 DSTM 节点建立 4over6 隧道，另一方面完成 IPv6 数据包的解封装，实现 IPv4 数据包在 IPv4 网络中的发送。反过来，接受从 IPv4 网络来的数据包，并通过 4over6 隧道传送给相应的 DSTM 节点。

（4）值得注意的问题

首先，DSTM 节点依据什么来决定是采用 IPv6 地址通信还是请求 DSTM 服务器为其分配 IPv4 地址，然后利用 IPv4 地址进行通信，这是一个值得考虑的问题。通常，是通过域名解析功能来获得目的端（网元）的 IP 地址类型的。那么在这种网络环境中域名解析过程是如何完成的呢？这可以有两种方式，这两种方式通常对应两种应用环境。在第一种应用环境中，DSTM 域中有 DNS 服务器，并且此 DNS 服务器能够支持 IPv4 地址对应的域名解析功能（同时也可以解析 IPv6 地址相关的域名，支持两种记录：A 记录和 AAAA 记录），则 DSTM 节点可以利用 IPv6 封装域名

解析请求，并从 DNS 服务器处获得域名对应的 IPv4 地址，然后 DSTM 节点再向 DSTM 服务器请求 IPv4 地址，实现与目的 IPv4 网元的通信。在第二种应用环境中，DSTM 域中没有 DNS 服务器，或者 DNS 服务器只支持 IPv6 地址对应的域名解析功能（只有 AAAA 记录）。在这种情况下，要求 DSTM 域内的 DNS 服务器可以和 DSTM 域外的 DNS 服务器之间进行 DNS 请求消息的翻译和转换，这个处理的过程较为复杂，具体内容可以参见 DNS-ALG 相关文档。

其次，由于 DSTM 服务器为 DSTM 节点分配的 IPv4 地址是临时的，在使用时间终结并且 DSTM 节点没有再提出继续使用的请求以后，DSTM 服务器将回收 IPv4 地址。这就造成 IPv4 网络中的网元在这段时间内不能和 DSTM 节点进行通信，也就是说 DSTM 节点可以单向主动与 IPv4 网络中的网元进行在通信，而 IPv4 网络中的网元不能主动与 DSTM 域中的 DSTM 节点通信。这种通信的单向性是 DSTM 的重要特点，这实际上也是所有采用临时地址分配策略的通信方式的共同问题。为了解决这个问题，提出了动态域名解析功能，DSTM 节点对应的域名是固定的，而域名对应的 IPv4 地址是临时的，这样，外部 IPv4 网络中的网元可以通过域名来确定 DSTM 节点的 IPv4 临时地址，从而实现双向通信功能。这种方式虽然解决了这种网络应用环境下的双向通信功能，但是同时增加了域名管理系统的管理和维护难度。首先，要求 DNS 服务器具有向 DSTM 服务器提出要求为 DSTM 节点分配 IPv4 临时地址的功能，这要求 DNS 服务器和 DSTM 处理流程均做相应的功能完善；其次，由于域名系统中的域名信息更新的频率较快，会造成域名系统不稳定，这反映在域名系统信息一致性可能存在问题，同时域名系统可能始终处于未收敛状态，从而形成域名空洞。动态 DNS 的研究也是目前域名研究方向的一个重要内容。

另外，当一个 DSTM 域中由于性能问题需要设置多个网关 TEP 时，这些 TEP 之间的信息应该能够共享，从而可以支持从一个 TEP 发出的 IPv4 流量，其相应的 IPv4 流量可以从另外的 TEP 接收。在多 TEP 方式下，网络的工作模式、TEP 之间的通信方式和内容等都是值得研究的内容，关于这个问题的研究在 IETF 中还没有得到足够的重视。

还有，DSTM 技术可能存在安全漏洞，DSTM 节点可以利用 TEF 作为中继来攻击 IPv4 网络中的网元。关于这一点，IETF 认为可以把 TEP 放在企业网或驻地网内部（防火墙之后），从而能够在一定程度上过滤掉来自网络内部的可疑流量。

## 3.6.2 隧道策略

隧道策略是 IPv4/v6 综合组网技术中经常使用到的一种机制。所谓“隧道”，简单地讲就是利用一种协议来传输另一种协议的数据的技术。在综合组网环境中，对于隧道类型的划分可以有多种依据。

按照隧道端点的网元类型，可以把隧道分为 R-R（路由器之间）、H-R（主机与

路由器之间，具体可以分为主机到路由器和路由器到主机两种）、H-H（主机之间）等几种。

按照隧道配置方法，可以把隧道分为手工配置隧道、自动配置隧道等。

按照隧道协议和承载协议的类型，可以把隧道分为 IPv4 over IPv6、IPv6 over IPv4、IPv4/v6 over MPLS 等几种。

按照数据的流动方向，可以把隧道分为单向隧道和双向隧道。

#### 1 应用方式

在综合组网环境中，隧道机制可以应用在骨干网和城域核心网中，同时也可以应用在企业网和用户驻地网中。

在综合组网的过程（网络过渡）中，当采用从边缘到骨干的过渡策略时，骨干网或城域核心网保持 IPv4 协议，而在网络边缘存在 IPv6 网络或 IPv6 主机，这些 IPv6 网元之间的通信可以利用隧道机制（IPv6 over IPv4 或 IPv4/v6 over MPLS）来实现。

在纯 IPv6 企业网和驻地网中，当存在 IPv4 主机或应用要和其他网络中的 IPv4 主机或应用通信时，需要在 IPv6 网中利用隧道机制来提供 IPv4 信息传输通道（IPv4 over IPv6）。同样，当纯 IPv4 网络中存在 IPv6 主机或应用的通信需求时，也可以采用隧道机制来提供 IPv6 信息传输通道（IPv6 over IPv4）。

#### 2. 基本原理

隧道包括隧道入口和隧道出口（隧道终点），这些隧道端点通常都是双栈节点。在隧道入口以一种协议的形式来对另外一种协议的数据进行封装并发送；在隧道出口对接收到的协议数据解封装，并做相应的处理。在隧道的入口通常要维护一些与隧道相关的信息，如记录隧道 MTU 等参数。在隧道的出口，通常出于安全性的考虑要对封装的数据进行过滤，以防止来自外部的恶意攻击。

隧道的配置方法包括手工配置隧道和自动隧道。而自动配置隧道又可以分为兼容地址自动隧道、6to4 隧道、6over4、ISATAP、MPLS 隧道、GRE 隧道等。这些隧道的实现原理和技术细节都不相同，相应地，其应用场景也就不同。

#### 3. 典型技术

（1）配置隧道

手工配置隧道主要应用在个别 IPv6 主机或网络需要通过 IPv4 网络进行通信的场合，这种方式的特点是实现相对简单；缺点是扩展性较差。当需要通信的 IPv6 主机或网络比较多时，隧道配置和维护的工作量较大。

手工配置隧道适合于综合组网的初期；同时在综合组网的后期，其也可以以“默认隧道”的方式而存在。

手工配置隧道的隧道终点的 IPv4 地址是从隧道入口的配置信息（通常是路由信息）里获得的。对于每一个隧道，隧道入口都必须保存该隧道终点的 IPv4 地址。当 IPv6 数据包通过这个隧道传输时，配置的隧道终点 IPv4 地址将作为封装数据包的目的地址。

（2）6to4 隧道

6to4 隧道是自动隧道的一种，也是 IETF 较为重视并得到深入研究、有广阔应用前景的一种网络过渡机制。

6to4 隧道的主要应用环境：它可以使连接到纯 IPv4 网络上的孤立的 IPv6 子网或 IPv6 站点与其他同类站点在尚未能获得纯 IPv6 连接时进行彼此间的通信。

采用 6to4 隧道的通信方式称为 6to4 过渡机制。通过这种方式，IPv6 可以获得相对于广域网络很高的独立性，可以跨越许多 IPv4 子网，使在 IPv4“海洋”中的 IPv6“孤岛”能相互连接。在 IPv4 网络内可以采用多种路由协议（OSPF/BGP/RIP/ISIS 等），两个 6to4 域之间可以通过 MP-BGP 路由方式实现路由可达。对于 6to4 机制的具体实现，只需要在边界路由器上增加配置，而对于主机，除了增加一个默认地址选择以外不需要其他修改。

6to4 隧道采用特殊的 IPv6 地址，IANA 为 6to4 过渡方案永久地分配了一个具有 IPv6 格式前缀 0x0002，表示成 IPv6 地址前缀的格式为 2002::/16。如果一个用户站点拥有至少一个有效的全球唯一的 32 位 IPv4 地址（v4ADDR），那么该用户站点将不需要任何分配申请即可拥有如下的 IPv6 地址前缀：2002:V4ADDR::/48。

在边界路由器上，IPv6 包将被封装在 IPv4 包里并通过隧道传输。在隧道起点封装时，边界路由器将提取出 6to4 地址中的 IPv4 地址作为隧道终点的地址。封装后的 IP 包到达目的 6to4 路由器时被解封装。站点的 IPv4 地址包含在 IPv6 地址前缀中，因此 IPv4 隧道的末端可从 IPv6 域的地址前缀中自动提取。

在过渡环境中，有两种情况需要考虑：一种是通信的双方都处于 6to4 域中，并且均采用 6to4 地址；另外一种情况是通信的一端处于 6to4 域中，并采用 6to4 地址，而另一端则处于纯 IPv6 域中，并采用纯 IPv6 地址。对于前一种情况，由于通信双方的 6to4 路由器都能识别并处理 6to4 封装，因此实现方式相对简单；对于后一种情况，则要求纯 IPv6 网络的网关能够在处理纯 IPv6 数据的同时，也能处理 6to4 数据，因此网关能够充当 6to4 中继器（中继路由器在其纯 IPv6 接口上参与 IPv6 单播路由协议，也可以同时在 6to4 伪接口上参与 IPv6 单播路由协议，但它们工作于相对独立的不同的路由域内；其还可以在支持 6to4 的 IPv4 接口上参与 IPv4 单播路由协议）。上述两种情况所对应的组网方式也略有不同。

6to4 隧道的优点是实现相对简单，支持的设备较多。其缺点是 6to4 机制在网络中的布置有一定的耦合性，当 6to4 域与纯 IPv6 进行通信时需要 6to4 中继器。

6to4 隧道作为一种隧道机制，同样也面临着相同的安全问题，但是由于有 6to4

中继器存在，使得问题更为复杂。关于 6to4 隧道的安全性分析参见 IETF RFC。

6to4 机制的一个值得重视的主要问题是：路由泄漏问题。所谓的路由泄漏是指，IPv4 域中的路由以 6to4 地址的形式泄漏到纯 IPv6 域的路由中。在采用 6to4 中继器的组网环境中，中继路由器必须向纯 IPv6 外部路由域通告一个到 2002::/16 的路由。这个到 2002::/16 的路由通告能在纯 IPv6 路由系统中传播多远则是一个至关重要的问题。选择不正确的策略将导致这个区域内存在潜在的不可达问题或糟糕的传输性能。为防止 IPv4 路由表成分混入 IPv6 路由表，不能将比 2002::/16 更精确的 6to4 前缀通告进入纯 IPv6 路由域中。因此，拥有纯 IPv6 连接的 6to4 站点不允许在该连接上通告有到 2002::/48 的路由，并且所有的纯 IPv6 网络必须过滤掉所有前缀长度大于/16 的 2002::路由公告。

（3）兼容地址自动隧道

兼容地址自动隧道是自动隧道的一种，在 IETF 的 RFC 中进行规定，但是目前已不推荐使用这种隧道方式。

兼容地址自动隧道可以应用在网络边缘，用于在 IPv4 网络有 IPv6 通信需求的双栈主机或终端（也可以是小型 IPv6 网络）之间进行通信的情况。

具有兼容地址自动隧道功能的 IPv6/IPv4 节点应该被分配一个 IPv4 兼容地址。IPv4 兼容地址是由 96 位的全零前缀和后 32 位的 IPv4 地址组成的。只有在准备接收封装在 IPv4 数据包里的目的地址内嵌着 IPv4 地址的 IPv6 数据包时，该节点才应该配置 IPv4 兼容地址，IPv4 封装数据包头中的目的地址等于 IPv6 数据包头中的 IPv4 兼容目的地址的低 32 位。

兼容地址自动隧道的终点地址是根据经过隧道的数据包来确定的。如果目的 IPv6 地址是 IPv4 兼容地址，这个数据包就能够通过自动隧道；如果目的 IPv6 地址是普通 IPv6 地址，则不能够通过自动隧道发送。

路由表项能够指导数据包的自动隧道。一种实现是前缀 0:0:0:0:0:0/96 有一个专门的静态路由表项，也就是说，这个路由将全零前缀来用作 96 位掩码。匹配这个前缀的数据包将被发送到能完成数据包自动隧道的伪接口。因为所有的 IPv4 兼容地址都匹配这个前缀，因此所有的数据包都会通过自动隧道发送到目的地。

这种自动隧道方式的实现相对较为简单（不像 DSTM 中需要为双栈节点动态分配 IPv4 地址），但是其缺点是：扩展性较差（需要为每个双栈主机分配 IPv4 兼容地址）、IPv4 地址消耗较大（由于兼容地址对应相应的 IPv4 地址，所以每一个需要通信的双栈主机都要静态分配一个 IPv4 地址）。基于上述原因，IETF 不推荐在网络过渡中采用上述方式，对于 IPv4 兼容地址的使用也持保守的态度。

作为隧道技术的一种，其也有着一定的安全隐患，隧道的终点可能受到来自不明主机的攻击。为了避免这种情况的发生，可以有如下策略：隧道入口过滤、隧道出口过滤、IPSEC 封装等。

（4）6over4

6over4 机制通常只能应用在网络边缘，如企业网和接入网。

6over4 使得没有直接与 IPv6 路由器相连的孤立的 IPv6 主机通过 IPv4 组播域作为它们的虚拟链路层形成 IPv6 的互连。如果需要实现 IPv6 的路由，就需要至少有一个使用 6over4 的 IPv6 路由器和该 6over4 主机连接在同一个 IPv4 的组播域中。使用该机制互连的主机并不需要 IPv4 兼容的地址或配置的隧道，通过这种机制，IPv6 可以独立于底层的链路，而且可以跨越支持组播的 IPv4 子网。

一个站点在 IPv6 过渡初期，可以将 IPv6 边界路由器的连接 IPv4 域的接口配置成支持 IPv6 over IPv4，在另一个连接 IPv6 域的接口上配置 IPv6。任何一个在 IPv4 域的支持 6over4 的主机都可以与这些路由器或 IPv6 域进行自由通信，而不需要手动配置隧道，也不需要 IPv4 兼容的地址的主机。

6over4 机制由于要求在 IPv4 网络中支持组播功能，而目前大多数网络均没有布置组播功能，因此其在实际应用中很少被利用。另外，IPv4 的组播特性作为虚拟链路层，是一种本地传送机制，因此其适用范围很小，只适用于双栈主机间的通信，不能解决将一个孤立的节点连接到全局 IPv6 网络中的问题。

（5）隧道代理

隧道代理通常应用于独立的小型的 IPv6 站点，特别是独立地分布在 IPv4 互联网中的 IPv6 主机需要连接到已有的 IPv6 网的情况。

隧道代理（TB）提供一种简化配置隧道的方法，可以减少繁重的隧道配置工作。隧道代理的思想就是通过提供专用的服务器作为隧道代理，自动管理用户发出的隧道请求。用户通过 Tunnel Broker 能够方便地和 IPv6 网络建立隧道连接，从而访问外部可用的 IPv6 资源。隧道代理这种过渡机制对于在 IPv6 的早期吸引更多的 IPv6 使用者方便快捷地实现 IPv6 连接有很大的益处，同时也为早期的 IPv6 提供商提供了一种非常简捷的接入方式。

（6）ISATAP

ISATAP 机制（the Intra-Site Automatic Tunnel Addressing Protocol，站内自动隧道寻址协议）在 IETF 的 RFC 中进行定义。

ISATAP 通常应用在网络边缘，如企业网或接入网。ISATAP 可以和 6to4 技术联合使用。

ISATAP 可以使 IPv4 站点内的双栈节点通过自动隧道接入 IPv6 路由器，允许与 IPv6 路由器不共享同一物理链路的双栈节点通过 IPv4 自动隧道将数据包送达 IPv6 下一跳。

ISATAP 过渡机制使用一个内嵌 IPv4 地址的 IPv6 地址，无论站点使用的是全球

的还是私有的 IPv4 地址，都可以在站点内使用 IPv6-in-IPv4 的自动隧道技术。ISATAP 地址格式既可以使用站点单播 IPv6 地址前缀，也可以使用全局单播 IPv6 地址前缀，即能支持站点和全局的 IPv6 路由。

（7）MPLS 隧道

MPLS 隧道主要应用于骨干网和城域核心网。

MPLS 隧道实现 IPv6 岛屿互连的方式，尤其适合已经开展了 BGP/MPLS VPN 业务的运营商。这种过渡方式可以使运营商暂时不必将现有核心网络升级为 IPv6 网络就可以对外提供 IPv6 业务。

IPv6 站点必须通过 CE 连接到一个或多个运行 MP-BGP 的双栈 PE 上，这些 PE 之间通过 MP-BGP 来交换 IPv6 的路由可达信息；通过隧道来传送 IPv6 数据包。

这种隧道方式的优点如下。

首先，其适合从边缘到核心的网络过渡策略，骨干网和城域核心网可以仍然保持原有的 IPv4 协议，而只是在网络的边缘通过 MPLS 技术来实现 IPv4 数据包和 IPv6 数据包的传送。

其次，其扩展性较好。当原有网络实现了 MPLS 时，各个边缘网络可以自主选择网络过渡时间和组网方式（本地网的组网方式不受 MPLS 隧道机制的影响）。

这种方式的主要缺点是：其实施是以网络中已经部署、实施了 MPLS 为前提条件的，对于尚没有部署 MPLS 的网络不适用。

（8）二层隧道

为了连接分散的 IPv6 网络，一种可能的方法是利用二层技术（如 ATM、PPP、L2TP 等）把这些 IPv6 网络连接在一起。

这种方式主要用来将少量的、相对重要的 IPv6 网络（孤岛）互连起来。

这种方式的优点是概念清晰、易于理解；这种方式的缺点是实现较为困难，扩展性较差，当需要互连的 IPv6 网络较多时，不宜采用这种方式。

### 4. 主要问题

上述的各种隧道技术有着一些需要重点分析的共性问题，它们对于分析综合组网有着重要的意义。

（1）MTU 问题

在隧道技术中，利用一种协议（承载协议）来传送另外一种协议（负载协议）封装的数据。承载协议（如 IPv4）形成的链路存在一个 MTU 值，当负载协议（如 IPv6）数据包的尺寸大于承载协议的 MTU 值减去承载协议的封装格式长度时，在隧道的入口处会出现负载协议数据包的拆分，在隧道出口处会出现负载协议数据包的

重组。这就增加了隧道出入口的实现复杂度。

具体地讲，当承载协议为 IPv4，而负载协议为 IPv6 时，如果仅考虑 IPv4 对数据包的处理，IPv6 的 MTU 可为（65535－20）字节（20 字节是 IPv4 报头的长度）。在隧道入口，当 IPv6 数据包长度超过这个 MTU 时，其向源端返回“数据包过长”的 ICMP 错误消息；当 IPv6 数据包小于这个 MTU 值，但是大于 IPv4 传输链路的 MTU 时，虽然也能够传送，但是这样大的 MTU 会带来一些问题：首先，这会导致 IPv6 数据包分段（当 IPv4 路径 MTU-20 小于 1280 字节时，仍存在数据包分段，因为 IPv6 协议规范中规定 IPv6 的任何链路层的 MTU 都必须大于等于 1280 字节）。一旦出现数据包丢失，重传的数据包将多于丢失数据包，会导致性能下降，因此应尽量避免 IPv4 层过多的数据包分段。其次，隧道中经过 IPv4 拆分的数据包在隧道终点需要重组，如果隧道终点是路由器，那么将消耗路由器上更多的内存进行数据包整合，重组成完整的 IPv6 数据包后才能继续转发。

解决上述问题的一个可能的方法是：首先，获得 IPv4 路径（隧道）的 MTU 值（具体方法参考 IPv4 路径 MTU 发现协议）；然后，在隧道入口处记录这个值（隧道路径上的 IPv4 路径 MTU）；再后，IPv6 的 MTU 发现协议工作时将考虑这个值，使得 IPv6 数据包的长度不大于 IPv4 路径 MTU-20 字节。这样可以避免 IPv6 数据包的分段，也简化了处理过程，提高了传输效率。

（2）安全问题

所有隧道技术均面临着安全问题，这种问题在自动隧道技术中更为复杂。

① 在隧道的入口处应该有一定的过滤功能，防止非法数据进入隧道，从而对隧道出口后面的网络造成攻击。

② 在隧道的出口处也应该有一定的过滤功能，防止非法数据进入本地网络。

③ 在隧道的出口和入口之间如何建立信任关系是一个值得考虑的问题。对于配置隧道来说，这可以利用多种认证方式来鉴权，并可以利用加密技术来传送数据（如 ESP、AH 等）。但是对于自动隧道，安全问题分析变得较为复杂，因为不能在每次传送数据时都进行身份认证，因此可能出现网络中其他网元利用身份伪装（模拟隧道入口后面的网络）方式对隧道出口后面的网络进行攻击的情况。

（3）路由问题

在隧道技术中，路由问题是需要重点分析的问题之一。概括起来讲，隧道的路由问题包括：路由方式的选择、路由泄漏、路由环回等方面。

① 在隧道技术中，路由方式的选择分为两种：一种是承载协议层的路由方式选择；另一种是负载协议层的路由方式的选择。这两种路由方式的选择有相对的独立性，可以根据网络规模、网络结构、自治域的组织等情况来自主选择，如 IPv6 自治域内部可采用 RIPng 或 OSPFv3 路由协议；在 IPv6 自治域之间，可采用 BGP4+路由

协议等。重点应该考虑如何利用承载协议来传送负载协议的路由信息，目前 MP-BGP 用来解决这个问题。

② 路由泄漏问题也是隧道技术分析中应该注意的问题。所谓的“路由泄漏”是指承载协议层的路由信息和负载协议层的路由信息进入对方的路由表中，从而造成路由信息膨胀、管理混乱、效率下降等问题。造成路由泄漏的根本原因是：在隧道机制中，尤其是自动隧道技术中采用了一些特殊的地址表示方法，如 6to4 地址、IPv4 兼容地址等，这些地址中均包含了 IPv4 地址信息，这些地址之间的路由信息传递时，有可能泄漏到纯 IPv6 网络的纯 IPv6 路由信息中，从而把 IPv4 路由信息引入 IPv6 路由表中（关于地址泄漏问题的具体例子在前面的 6to4 技术分析中已经提过）。解决这个问题的一种思路是：严格限制这些与特殊地址类型相关的 IPv6 路由的传播。例如，为防止 IPv4 路由表成分混入 IPv6 路由表，不能将比 2002::/16 更精确的 6to4 前缀通告进入纯 IPv6 路由域中，并且所有的纯 IPv6 网络必须过滤掉所有前缀长度大于/16 的 2002::路由公告。

③ 地址环回问题也应该在隧道技术的路由分析中给予一定的注意。一般来讲，负载协议层的路由本身、承载协议层的路由本身在路由协议设计时已经考虑了路由问题，因此不会出现路由环回问题。但是在自动隧道技术中，由于牵涉两类 IPv6 地址（纯 IPv6 地址和特殊 IPv6 地址），可能会出现路由环回问题。路由环回问题是路由泄漏问题的副产品，当出现路由泄漏问题时，会造成路由信息的混乱，从而引起路由环回。解决了路由泄漏问题也就解决了路由环回问题。

（4）QoS 问题

关于隧道技术所带来的 QOS 问题，可以从以下几个方面来分析。

① 在隧道技术中，当 IPv6 数据利用 IPv4 隧道来传送时，经过隧道 IPv6 的跳数减一，而实际上已经经历了 IPv4 域内的多跳，这增加了 IPv6 层面的 QoS 管理的难度。

② IPv6 协议自身增加了一些 QoS 方面的考虑，如在 IPv6 包头中定义了 1 个 4 比特的优先级区域，可以指示 16 种优先级别；在 IPv6 的包头中定义了 1 个 24 比特的信息流标签，路由器不需要检查地址、端口或其他信息，就可以按流标识进行相应的处理。但是由于 IPv4 隧道的存在，使得 IPv6 的上述 QoS 机制的应用效果受到影响，主要原因是 IPv4 隧道部分的 QoS 无法保证。解决这个问题的一个思路是定义 IPv6 的优先级字段值与 IPv4 隧道优先级之间的映射关系，使得高优先级的 IPv6 数据仍然可以在 IPv4 隧道中得到优先处理，从而一定程度上保证 IPv6 数据的性能。

（5）扩展性问题

各种隧道技术均需要隧道入口和隧道出口两个部分，是成对使用的，一般来说，它们分别处于不同的网络之中，当使用某一种隧道技术时，要求这两个网络（至少

是边界路由器）均支持这种技术，因此这两个网络的组网技术的选择存在着一定的耦合性。这种耦合性直接制约了技术的扩展性。为了支持多个不同网络的互连，需要增加边界路由器的功能，但是这会增加成本和实现的难度。

5. 技术总结

目前，静态配置隧道和二层隧道用于将个别的 IPv6 网络通过 IPv4 网络连入更大的 IPv6 网络，但是鉴于组织、管理、维护的难度，不利于大规模使用。

6to4 隧道、MPLS 隧道可以用在骨干网和城域核心网中，实现不同 IPv6 网络（或主机终端）的互连。

隧道代理技术可以应用在网络边缘，实现 IPv6 网络与 IPv6 核心网络的互连。

ISATAP 与 6to4 相结合用来组建企业网和专用网络。

6over4 机制、IPv4 兼容地址自动隧道机制在 IPv4/v6 综合组网中不推荐使用。

## 3.6.3 翻译策略

双栈策略解决了 IPv6 与 IPv4 的共存问题，其实现原理是在网元（如主机）中实现两个协议栈，可以根据应用的需要来选择合适的协议栈与外部通信（具体分析见前面的相关内容）。但是在网络的过渡时期不可能要求所有的主机或终端都升级支持双栈，在网络中必然存在纯 IPv4 主机和纯 IPv6 主机之间进行通信的需求，由于协议栈不同，很自然地需要对这些协议进行翻译转换。

对协议的翻译涉及两个方面，一方面是 IPv4 与 IPv6 协议层的翻译；另一个方面是 IPv4 应用与 IPv6 应用之间的翻译。

在分析翻译策略时需要考虑两个重要的问题：一个是翻译点的选择问题；另一个是翻译策略对综合组网的网络结构的影响。

对于前者，一般来说，由于骨干网络的处理逻辑要求尽量简单，从而提高处理效率，因此翻译点不能选在骨干网络或核心网络中。由于不能在骨干网和核心网络进行翻译处理，因此翻译策略只能应用在网络的汇聚层面或主机终端处，在 IETF 中，分别有相应的技术对应汇聚层面的翻译处理（NAT-PT、TRT）和主机终端层面的翻译处理（BIS、BIA）。

对于后者，由于进行翻译处理时需要保留一些状态信息或相关的处理参数，因此要求从某个翻译点出去的数据还要从这个点返回，否则将不能完成翻译功能而进行正常的通信。目前关于多个翻译点之间如何组织、如何协同工作的研究还比较少，是一个值得关注的研究方向。

另外，采用翻译策略破坏了 IPv4 主机与 IPv6 主机之间的端到端的通信，使得一些服务（如安全）和业务的正常运行受到影响。目前对这一问题的研究相对较多，如 IPSEC 的 NAT 穿越问题、各种业务的 NAT 穿越问题等，针对这些问题也提出了

一些解决思路，但是这些思路的对应方法实现复杂，而且扩展性较差。因此这个方向还需要进一步的深入研究，但是应该说其研究空间并不是很大。

### 1. 典型技术

翻译策略可以对应多种实现技术，其中 NAT-PT 和 TRT 主要应用于网络汇聚层；而 BIA、BIS 则主要是针对主机终端而提出的。

（1）NAT-PT

为了解决纯 IPv4 节点与 IPv6 节点之间的通信，IETF 提出了地址/协议转化方案 NAT-PT。关于应用 NAT-PT 的一个基本假设是：IPv6 域和 IPv4 域之间没有其他的方法（如本地 IPv6 连接、各种隧道）来为 IPv6 和 IPv4 节点提供相互通信时，才使用 NAT-PT 过渡机制。也就是说，NAT-PT 过渡机制用于纯 IPv6 节点和纯 IPv4 节点之间的相互通信，应该避免在纯 IPv6 节点和一个双栈节点的 IPv4 部分之间使用协议翻译。

地址/协议转换采用了直接明了的转化方式，不用修改上层协议即能互相通信。该方案的关键设备又称为 NAT-PT 网关，能够实现 IPv4 和 IPv6 协议栈的互相转换，包括网络层协议、传输层协议及一些应用层协议之间的互相转换。

具体地讲，NAT-PT 包括如下三个功能模块：SIIT 协议翻译功能（IETF RFC 2765）、NAT 的动态地址翻译能力及相应的应用层网关（ALG）。其中，SIIT 协议翻译功能（SIIT——无状态 IP/ICMP 翻译算法）定义了 IPv4 包与 IPv6 包之间的相互翻译的过程，主要是字段的映射关系及相关参数的确定方法，但是它没有给出如何在翻译的过程获得 IPv4 临时地址；而 NAT 的动态地址翻译功能解决了这个问题，它维护一个 IPv4 地址池并负责临时 IPv4 地址的分配，还要维护与翻译过程相关的信息；SITT 和 NAT 合作能够完成 IPv4 包和 IPv6 之间的翻译，但是对于封装在 IPv4 或 IPv6 包中的上层应用信息则无能为力，而应用层网关 ALG 正是为解决这个问题而提出的，它可以基于应用对 UDP 或 TCP 中的高层应用进行翻译，通常不同的应用要有不同的应用层网关（如 DNS-ALG 及其他业务的 ALG 等）。上述三个功能相互结合能够完成从应用层面到网络层面的信息翻译工作，因此 NAT-PT 为实现大量常用的应用程序能在纯 IPv6 节点和纯 IPv4 节点之间互通提供了相对完整的解决方案。

地址/协议转换技术较好地解决了 IPv4 和 IPv6 的互通问题，其最大优点是原有的各种协议不加改动就能与新的协议互通。但该技术在应用上有一些限制：首先，在拓扑结构上要求一次会话中所有数据包的转换都在同一个路由器上完成，因此地址/协议转换方法比较适用于只有一个路由器出口的网络；其次，一些协议字段在转换时不能完全保持原有的含义；另外，协议转换方法缺乏端到端的安全性（IPSEC 穿越问题依然没有很好地解决）。

（2）TRT

传输中继转换器简称 TRT（Transport Relay Translator），适用于纯 IPv6 网络与纯 IPv4 网络通信的环境。TRT 系统位于纯 IPv6 主机和纯 IPv4 主机之间，可以实现 {TCP，UDP}/IPv6 与 {TCP，UDP}/IPv4 的数据的对译。传输中继可以分为两类：TCP 中继和 UDP 中继。

TRT 与 NAT-PT 的最大区别是：TRT 作为中继，在 TCP/UDP 层面以代理的身份来沟通双方，如 TCP 中继分别与 TCP 通信的双方建立 TCP 连接，双方的所有 TCP 通信均由 TCP 中继来中转。而 NAT-PT 则只起翻译作用，并不代理通信。

TRT 的优点主要表现在：TRT 不需要修改纯 IPv6 主机和纯 IPv4 主机；TRT 不需要考虑 PMTU 和数据包分片的问题。

TRT 的不足如下所述：TRT 只支持双向传送，不支持单向的多播数据数据包的转换；TRT 是一个位于两个通信实体中间的有状态的传输中继转换系统，即使在同一个区域部署多个 TRT 系统，一个传输层会话也必须通过同一个 TRT 系统；TRT 系统本身无法进行非 NAT 友好协议的转化，如 IPsec 等。

以下描述假定所有业务都是由 IPv6 主机发起的，目的是 IPv4 主机。如果使用合适的地址映射机制，TRT 也可以支持 IPv4 到 IPv6 的数据业务。

（3）BIS

上面介绍的 NAT-PT 和 TRT 技术均应用在网络汇聚层，而 BIS 和 BIA 则应用在主机和终端处。

BIS 技术是在双栈主机中添加若干个模块（翻译器、扩展域名解析器、地址映射器），用于监测 TCP/IP 模块与网卡驱动程序之间的数据流，并进行相应的 IPv4 与 IPv6 数据包之间的相互翻译。

当与其他 IPv6 主机进行通信时，在这台主机内部给对应 IPv6 主机分配一些 IPv4 地址，这些地址只在这台主机内部使用。而且，这种分配过程是通过 DNS 协议自动完成的。所以，用户不用关心与其通信的对应主机是不是 IPv6 主机。也就是说，主机可以使用现有的 IPv4 应用和其他 IPv6 主机进行通信，使其成为能够既支持 IPv4 应用又支持 IPv6 应用的双栈主机，从而扩大了双栈主机的应用领域。

具体地讲，当翻译器收到来自 IPv4 应用的数据包时，将 IPv4 头转换为 IPv6 头，然后对转换后的数据包进行适当的分段处理（因为 IPv6 头至少比 IPv4 头大 20 字节），发送到 IPv6 的网络中。当从 IPv6 的网络中接收到 IPv6 的数据包时，翻译器做相反的转换，但此时不对数据包进行分段处理。扩展域名解析器用于对来自 IPv4 应用的请求返回一个正确的响应。地址映射器负责管理一个 IPv4 地址池，这个地址池里也可以包含私用地址。同时，地址映射器维护一张包含 IPv4 和 IPv6 地址对的映射表。当解析器和翻译器需要为一个 IPv6 地址分配一个 IPv4 的地址时，地址映射器从其

管理的地址池中选出一个 IPv4 地址，并在映射表中动态地记录下地址之间的映射关系。

另外，BIS 机制可以和其他转换机制共存。

（4）BIA

BIA 技术在双栈主机的 Socket API 模块与 TCP/IP 模块之间加入一个 API 翻译器，所以它能够在 IPv4 的 Socket API 函数和 IPv6 的 Socket API 函数间进行互译。这种机制简化了 IPv4 和 IPv6 间的转换，但无须进行 IP 头的翻译。

采用 BIA 的双栈主机假定在本地节点上同时存在 TCP/IPv4 和 TCP/IPv6 两种协议栈。

当双栈主机上的 IPv4 应用程序与其他 IPv6 主机通信时，API 翻译器检测到 IPv4 应用程序中的 Socket API 函数，并调用 IPv6 的 Socket API 函数与 IPv6 主机通信，反之亦然。为了支持 IPv4 应用程序与目标 IPv6 主机间的通信，在 API 翻译器中，IPv4 地址池由域名解析器进行分配。

### 2. 问题讨论

上面对翻译机制进行了简单的介绍，主要侧重于实现原理、应用场景等方面。实际上翻译机制所牵涉的内容较多，如安全问题、效率问题、双向通信问题等。但是有一些问题是共性的，对这些问题的分析有利于对翻译机制的理解及对综合组网技术的深入分析。

（1）翻译策略的应用环境

上面已经分析了不同翻译技术的应用环境，可以总结一下：① 在核心网中不应该应用翻译策略；② 在汇聚层和主机终端均可以采用翻译策略，并且它们不相互矛盾；③ 翻译策略的应用是不得已而为之的下策，能不用最好不用，因为其对性能有较大影响，也制约了网络的扩展性。

（2）MTU 问题

IPv4 和 IPv6 的区别之一是在 IPv6 中路径 MTU 发现是必需的，但在 IPv4 中这是可选的，这意味着 IPv6 路由器不会分解数据包，只有发送方才会做分段。

如果 IPv4 节点做路径 MTU 发现（这通过对包头部的 DF 位进行设置可以实现），路径 MTU 发现就可以进行端到端操作，也就是要通过翻译器。在这种情况下，IPv4 和 IPv6 路由器都会发送 ICMP 包“数据包过大”消息回给发送方。当 IPv6 路由器发送的 ICMP 错误消息将通过翻译器时，翻译器就会将这些 ICMP 错误消息翻译成 IPv4 发送方可以理解的形式。在这种情况下，只有到达翻译器的 IPv4 数据包已经分段，对应的翻译数据包才会有 IPv6 分段头部。

如果 IPv4 发送方不进行路径 MTU 发现操作，翻译器就不得不确保数据包不会超过 IPv6 侧的路径最大传输单元，由于 IPv6 保证了 1280 字节的数据包不需要分段，所以也可以通过分解 IPv4 数据包，让它匹配 IPv6 数据包的 1280 字节来实现。这也就是说，当 IPv4 发送方不进行路径最大传输单元发现操作时，翻译器就必须一直带有 IPv6 分段头部来表明发送方允许分段操作。

# 第 4 章 IPv6 技术产业发展情况

**本章要点**

- ✓ 全球 IPv6 发展情况
- ✓ 我国 IPv6 发展情况
- ✓ 我国 IPv6 过渡方案


近年来，全球下一代互联网产业呈现加速发展态势。各发达国家和地区纷纷出台国家战略层面的规划和布局，都在抓住下一代互联网这个战略必争之地，做出国家力量的部署，下一代互联网网络建设逐步由实验网转向商用，重要标准、关键设备、软件和系统研发趋于成熟，并开始规模化实验与应用。

# 4.1 全球 IPv6 发展情况

## 4.1.1 地址资源分布状况

### 1. IPv4 地址资源已分配完，我国 IPv4 地址资源相对匮乏

2011 年 2 月 3 日，全球 IP 地址分配机构 IANA（互联网编号分配机构）宣布其地址池中的 IPv4 地址已分配完。2011 年 4 月 15 日，亚洲地区 IP 地址分配机构 APNIC（亚太互联网络信息中心）进入最后一个/8 IPv4 地址块的分配，根据 APNIC 相关政策，此后其会员每次申请最多可获得一个/22 的 IPv4 地址块（1024 个 IPv4 地址）。其他地区性 IP 地址分配机构包括 RIPE NCC（欧洲）和 ARIN（北美）预计也将分别在 2012 年和 2013 年分配完可用的 IPv4 地址资源。

截至 2011 年 12 月底，我国网民数达到 5.13 亿人，互联网普及率仅为 38.3%，拥有的 IPv4 地址数量为 3.30 亿个（不含港澳台地区）[①]，在国家和地区中排名第二，占全球可用 IPv4 地址总量的 7.72%，人均 IPv4 地址拥有量仅为 0.24 个。另据工信部电信研究院的研究报告，未来 5 年我国 IP 需求量为 345 亿[②]个。IP 地址严重不足，将成为制约我国物联网、移动互联网、云计算、三网融合发展的瓶颈，即使大量应用地址翻译（NAT）等技术延缓 IPv4 地址消耗，仍不能满足快速增长的应用需求，还会显著增加网络复杂性和管理难度，降低网络与信息安全水平和服务质量。

① 数据来源：中国互联网络信息中心（CNNIC）发布的《第 29 次中国互联网络发展状况调查统计报告》。

② 未来 5 年我国 IP 需求量为 345 亿个，其中移动互联网为 10 亿个，物联网预计需求量为 100 亿个，固定互联网为 5 亿个，并且按照 IP 地址 33%的利用率来推算。

2. 全球 IPv6 地址资源分配提速，我国申请数量位居全球第五

截至 2012 年 3 月底，全球共有 196 个国家申请获得 IPv6 地址，其中拥有量最多的国家依次是巴西、美国、日本、德国、中国等。中国拥有的 IPv6 地址数为 9410 个（/32），约为巴西 IPv6 地址的 1/7、美国 IPv6 地址的 1/2，在国家和地区中排名第五，占全球已分配 IPv6 地址总量的 5.66%[①]。我国 IPv6 地址集中在 2011 年 7 月份以后获得，其中中国移动于 2011 年 8 月获得了一个/20 的 IPv6 地址块，中国电信于 2011 年 12 月获得了大小分别为/21、/22、/23、/24 的 4 个 IPv6 地址块，中国联通于 2011 年 7 月获得了/22 的 IPv6 地址块。

## 4.1.2　IPv6 支持能力

从 20 世纪末开始，全球建设了大量 IPv6 试验网，其中规模较大的网络包括美国 Internet2、欧洲 GÉANT2、亚太 APAN 和跨欧亚 TEIN2 及我国的 CNGI。目前这些试验网已经实现高速互连，形成了国际 IPv6 下一代互联网大规模试验网。商用方面，日本已有十余家运营商开展了 IPv6 的运营实践。其中 NTT 已建成全球性 IPv6 骨干网，还在本土开展基于 IPv6 的 IPTV 业务。美国最大的有线电视运营商 Comcast 从 2010 年第二季度开始为用户提供 IPv6 服务。欧洲西班牙电信、法国电信等也相继开展基于 IPv6 的服务。

截至 2012 年 3 月底，全球已分配的 IPv6 地址量占 IPv6 地址总量的 3.13%，其中通告的地址数量为 19.37%。全球活跃的 IPv6 BGP 路由数为 8641 条[②]。

活跃 IPv6 BGP 路由增长情况如图 4-1 所示。

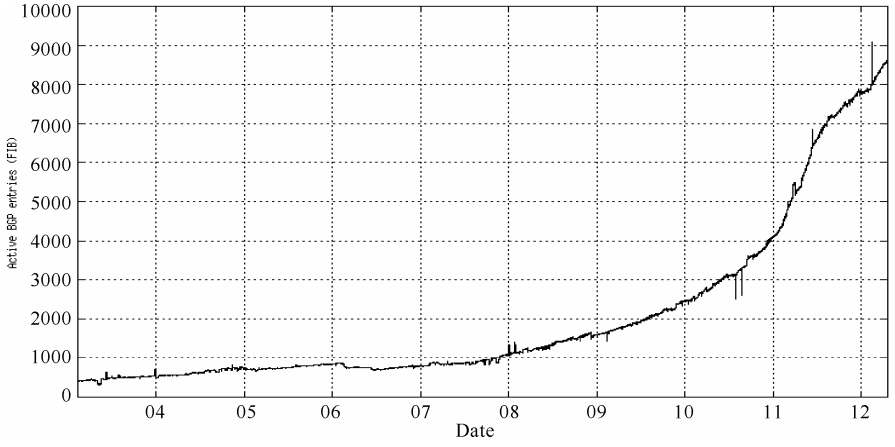
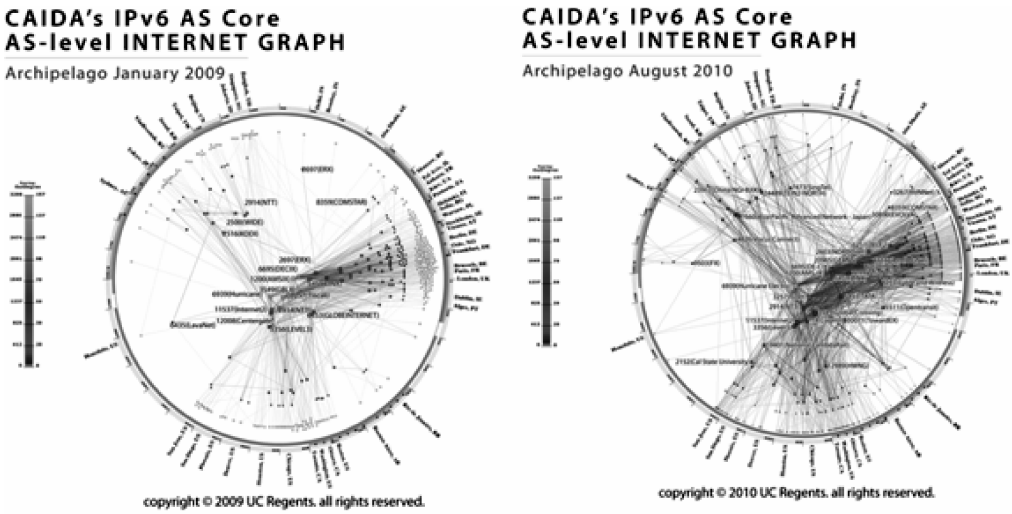



图 4-1　活跃 IPv6 BGP 路由增长

① 数据来源：http://resources.potaroo.net/iso3166/v6cc.html。

② 数据来源：http://bgp.potaroo.net/v6/as2.0/index.html。

加州大学圣地亚哥分校（UCSD）互联网数据分析合作协会（CAIDA）最新公布的 IPv6 自治域系统（AS）拓扑图如图 4-2 所示。截止到 2010 年 8 月，共有 21 852 个 IPv6 连接，715 个自治系统[①]。




（a）2009年1月IPv6全球地图　　（b）2010年8月IPv6全球地图

图 4-2　IPv6 全球地图

截至 2011 年 12 月，全球 13 个域名系统（DNS）根服务器中共有 9 个添加了有效的 AAAA 记录（指向 IPv6 地址的记录），分别为 A、D、F、H、I、J、K、L、M 根服务器；全球 315 个顶级域名服务器中支持 IPv6 的共有 267 个，占比 84.76%。

截至 2012 年 1 月，全球已经有 480 余款产品通过 IPv6 Ready Phase1 认证，670 余款产品通过 Phase2 认证[②]。总体上看，IPv6 产品类型十分丰富，覆盖了 IPv4 产品类型，并且取得了一定规模的应用。获得 IPv6 可用认证（IPv6 Enabled）的网络服务提供商（ISP）共有 131 家，其中马来西亚最多，共有 13 家 ISP 获得认证，中国共有 4 家 ISP 获得认证；获得 IPv6 可用认证的网站共有 1414 个，其中中国最多，共有 306 家，占比达 21.64%。另据国外媒体报道，由互联网性能监测公司 Measurement Factory 负责实施的一项针对 IPv6 网站的调查统计结果显示，在过去 12 个月中，支持 IPv6 技术的.com、.net 和.org 网站数量已增长了 1900%，占比达到 25.4%，远远高于去年的 1.27%。这个数字的“巨大增长”主要得益于美国域名注册服务机构 Go Daddy 对 IPv6 的支持。

IETF 是国际 IPv6 标准化的主体，已制定 200 余项 IPv6 相关标准，核心标准体

① 数据来源：http://www.caida.org/research/topology/as_core_network/historical.xml。

② IPv6 论坛. IPv6 Ready 认证（IPv6 Ready）主要包括两个阶段：第一阶段（Phase-1）主要对 IPv6 核心协议的一致性和互通性进行测试；第二阶段（Phase-2）增加了可选协议测试。

系已经形成，目前主要工作集中于过渡技术及已有标准的完善上。除 IETF 之外，其他国际组织，如 ITU-T、3GPP、IEEE 等，也参与了 IPv6 相关标准的制定。ITU-T 侧重于 IPv6 应用于 NGN 的场景和需求，3GPP 则侧重于 IPv6 应用与 3G/LTE 的承载及业务应用。IEEE 侧重于无线局域网、智能电网、绿色节能等领域的 IPv6 应用标准化工作。

此外，根据《IPv6 全球部署评估报告》2011 年调查数据显示，约 1600 名国际调查对象（超过一半的被调查者为互联网服务供应商）中超过 70%计划 2012 年年底为其网络部署 IPv6。此次调查表明 IPv6 在被认可、规划和实际部署方面取得了积极的进展。

## 4.1.3　各国政府对 IPv6 发展的态度

近两年，全球下一代互联网产业呈现加速发展的态势，各发达国家和地区纷纷出台国家战略层面的规划和布局。

### 1. 美国

当前，美国采用了以军事和政府为先导的 IPv6 发展策略，从军事、政务、商业三个方面同时推进 IPv6 部署，并由国防部、预算管理办公室、商务部分别负责。

2003 年 6 月，美国国防部发布了一份关于向 IPv6 过渡的备忘录，并制定了“全球信息网格计划”等相关政策。根据 IPv6.com 网站资料，美国军方将全面部署 IPv6 的日期推迟到 2012 年。

美国预算管理办公室（OMB，Office of Management and Budget）主要负责政务网络向 IPv6 的迁移。2010 年 9 月，美国政府发布 IPv6 行动计划，并颁布 IPv6 推进工作组工作时间表明细，要求所有美国政府机构在 2012 年年底前把面向公众的网站和服务升级到支持 IPv6（包括 Web、E-mail、DNS、ISP 服务等），在 2014 年年底前实现与公众互联网及企业网相关应用软件的 IPv6 升级。

美国商务部负责商业和私营网络的 IPv6 推进，其下属电信和信息管理局（NTIA）则是具体实施单位。2010 年 9 月，NTIA 召集 Google、Verizon、Comcast、VeriSign、ISOC（国际互联网协会）等企业和机构共同讨论 IPv6 推进问题。此外，NTIA 还大力推进美国的宽带战略，支持示范网络建设，为 IPv6 业务的发展提供基础设施保证。

2012 年 9 月 30 日是美国联邦政府机构在公共网站和网络服务中支持 IPv6 的最后期限，有 1 万多家网站受到这一行政命令的影响，有助于推动 IPv6 在美国的部署。

### 2. 欧盟

2008 年 5 月，欧洲议会、经济和社会委员会、区域委员会共同发表“欧洲部署 IPv6 行动计划”，要求在欧洲范围内采取及时、高效、协调一致的行动，实现部署目

标。欧盟 IPv6 路线图计划到 2010 年年底实现 25%的企业、政府机构和家庭用户迁移至 IPv6。但是，这一目标未能实现，欧盟范围内的使用率约为 8%。

当前，欧盟推进 IPv6 发展的政策措施主要包括：通过开发大规模实验床建立示范工程，推动解决 IPv4 与 IPv6 的互联互通问题；推进政府采购，通过政府采购促进和带动 IPv6 的发展，使政府率先全面使用 IPv6；开展国际合作，欧盟正在与美国、日本、中国等国家和地区开展关于 IPv6 的项目合作，并且不断寻求新的合作机会。

#### 3. 日本

为实现向 IPv6 的平稳过渡，日本政府建立“官民共同推进体制”。在“E-Japan”战略中，将 IPv6 作为重要组成部分。2007 年 8 月，日本总务省成立了“互联网向 IPv6 过渡调查研究委员会”，形成了日本的 IPv6 过渡计划。2009 年 10 月，由日本总务省、JPNIC、电信和互联网运营商协会成立“日本 IPv4 地址枯竭工作组”，发布《IPv6 行动计划》，决定从 2011 年 4 月全面启动 IPv6 服务，目前已有 11 家 ISP 提供 IPv6 商用服务。

#### 4. 韩国

2010 年 9 月，韩国通信委员会召开了关于创建“下一代互联网协议（IPv6）促进计划”会议，并宣布从 2011 年 6 月开始，韩国国内的互联网、IPTV、3G 等移动通信服务都将启用下一代互联网协议 IPv6。韩国政府曾宣布 2011 年 6 月禁用 IPv4，全面部署 IPv6，然而，没有进一步消息证实韩国成功实现 IPv6 对 IPv4 的全面替代。

总体而言，各个国家和地区从 IPv4 向 IPv6 转换的步伐相差悬殊，据国际互联网工程任务组（IETF）公布的结果，目前日本的转换步伐最快。日本 NTT 电信服务商在 2011 年 6 月就已提供 IPv6 的商业服务。而美国政府则计划在 2012 年 9 月底前提供 WWW、E-mail、DNS 等 IPv6 服务，2014 年 9 月底前才提供基础网络与系统的 IPv6 服务。韩国网络服务商则计划在 2013 年提供 IPv6 服务。在欧洲，法国今年则先以政府部门网络转换 IPv6 为主，陆续才会提供 IPv6 的相关服务。整体而言，各国 IPv6 转换时间大都在 2012 年或之后。

### 4.1.4 产业界积极协作

面临 IPv4 耗尽的严峻形势，全球互联网产业界正在积极协作，合力推动 IPv6 的部署。2011 年 6 月 8 日，ISOC 连同 Google、Facebook、雅虎、Limelight Networks 等 1000 多家企业和机构发起 “世界 IPv6 日”活动，首次在全球范围内进行了 24 小时的 IPv6 规模试验，推广 IPv6 商业应用和发现潜在的技术问题。

2012 年 6 月 6 日，全球将再次举行主题为“World IPv6 Launch”的 “世界 IPv6 日”活动。ISOC 表示，届时，包括 AT&T、Comcast、Free Telecom、Internode、KDDI、

Time Warner Cable 及 XS4ALL 在内的 ISP 都在当天启用 IPv6 服务。另外，Facebook、Google、Yahoo 及微软的 Bing 等网站也自该日起永久启用 IPv6 支持，这意味着全球正式开展 IPv6 部署。

## 4.2　我国 IPv6 发展情况

我国较早开展了下一代互联网的研究，实施了一系列国家级技术创新计划、应用示范和试商用工程，已经取得了举世瞩目的成绩。在网络建设方面，建成世界上最大的 IPv6 网络；在设备研发方面，基本掌握了 IPv6 关键网络设备的核心技术，实现了产业化；在业务应用方面，开展业务系统的研发及新业务的应用示范；在技术创新方面，取得网络过渡、安全机制等方面的局部突破，这些都为我国下一代互联网实现跨越式发展提供了难得的历史机遇。

### 4.2.1　政府明确了 IPv6 发展路线图和时间表

下一代互联网已成为我国战略新兴产业的重要组成部分。在 2011 年 3 月国家最新颁布的《国民经济和社会发展第十二个五年规划纲要》中已明确指出，要重点发展下一代互联网等新一代信息基础产业，实施相关战略性新兴产业创新发展工程，推动相关重点领域跨越式发展，从而实现转型升级和提高产业核心竞争力。

2011 年 12 月 23 日，国务院总理主持召开国务院常务会议，研究部署加快发展我国下一代互联网产业。会议指出，抓住新形势下技术变革和产业发展的历史机遇，在现有互联网基础上进行创新，发展地址资源足够丰富、先进节能、安全可信，具有良好的可扩展性和成熟的商业模式的下一代互联网。会议明确了我国发展下一代互联网的路线图和主要目标，即 2013 年年底前，开展 IPv6 网络小规模商用试点，形成成熟的商业模式和技术演进路线；2014 年至 2015 年，开展大规模部署和商用，实现 IPv4 和 IPv6 主流业务互通。

为贯彻落实国务院常务会议精神，发改委等八部委联合编制了《关于下一代互联网“十二五”发展建设的意见》（以下简称为《意见》），在该《意见》中明确提出了我国下一代互联网“十二五”期间的发展目标：互联网普及率达到 45%以上，推动实现三网融合，IPv6 宽带接入用户数超过 2500 万，实现 IPv4 和 IPv6 主流业务互通，IPv6 地址获取量占全球已分配数量的 10%以上。下一代互联网理论研究、软件研发、设备制造、应用服务等领域实现高端突破，业务应用和终端设备对网络的支持能力显著提高，以自主技术为基础形成系统的国内和国际标准体系，国际标准提案数量增长 75%以上。建成较为完善的网络与信息安全保障体系，网络与信息安全水平、监管能力和管理话语权显著提升。网络单位信息流量综合能耗下降 40%以上，

网络设备制造产业万元增加值能耗下降 15%以上。关键领域自主产品国内市场占有率达到 80%以上，形成一批具有较强国际影响力的下一代互联网研究机构和骨干企业，新增就业岗位 300 万个，进一步增强对消费、投资、出口的拉动作用及对信息产业、高技术服务业、经济社会发展的辐射带动作用。为实现上述目标，发改委发布了两个重大专项，即下一代互联网信息安全专项和下一代互联网技术研发、产业化和规模商用专项。

## 4.2.2 国家项目积极支持与推动 IPv6 发展

国家十分重视下一代互联网的发展，有关部委组织实施了一系列与下一代互联网有关的工程和专项。

### 1. 高技术产业发展项目

在国家发展改革委的高技术产业发展项目中，2003 年国家发展改革委联合教育部、科技部、信息产业部、中国科学院、中国工程院、国家自然科学基金委等部委组织产学研各界启动了中国下一代互联网示范工程 CNGI，部署建设了 6 个主干网（覆盖全国 22 个城市、连接 59 个核心节点）、2 个国内/国际交换中心（北京和上海）、273 个驻地网。2005 年和 2006 年共设立 103 个 CNGI 技术试验及产业化项目，其中技术试验、应用示范和标准研究项目共 56 个，系统研发及产业化项目共 47 个。2008 年年底开始，组织实施 CNGI 试商用项目，包括列入国家拉动内需计划的“教育科研基础设施 IPv6 技术升级和示范应用”重大项目，以及 46 个业务试商用及产业化项目。来自国内上百所高校、上百个科研机构、所有全国性电信运营商、几十个设备制造商和软件开发商的上万人参加了上述工程建设，建成了大规模下一代互联网 CNGI 示范网络，提供了重大科研和新型业务的试验床，推动了标准制定和国产网络设备产业化，取得了大量示范性应用成果，增强了下一代互联网领域的自主创新能力，锻炼和培养了一批下一代互联网专业人才。

### 2. 创新能力建设项目

在国家发展改革委创新能力建设项目中，部署建设了下一代互联网领域的关于核心网、接入系统、互连设备和宽带业务应用等技术的国家工程实验室，为下一代互联网产业发展提供创新技术、标准和人才，使其成为下一代互联网产业共性技术的研发创新平台。

### 3. 科技重大专项

在“新一代宽带无线移动通信网”重大专项中部署了 SAE（系统架构演进）、移动业务控制网络、新型 IP 承载网架构、新型业务应用开发、终端与用户卡关键技术

研发等方面的研究和产业化课题。专项从顶层设计和总体规划入手，部署了无线泛在网络架构和总体设计、移动互联网总体架构、移动应用平台架构、移动网络与信息安全架构等研究课题。

#### 4. 重点科技工程

科技部在“十五”期间启动重点科技工程项目“高性能宽带信息网（3TNet）”。该项目以自主研制的 T 比特级的传输、路由和交换设备在上海地区（并扩展至长三角地区）建成了可运营级的、能支持大规模并发流媒体业务和交互式多媒体业务的高性能宽带信息示范网。目前以“高性能宽带信息网”为支撑，正在开发适合“三网融合”的、有线无线相结合、全程全网的中国下一代广播电视网（NGB）体系结构和关键技术。

科技部在“十一五”期间启动了“新一代高可信互联网”重点专项，包括：863 计划“新一代高可信网络”，通过设置“未来分组数据网络（FPBN）”等项目，构建一个柔性可重构、实现“三网融合”、跨区域的国家网络新技术试验网络；科技支撑计划项目“可信任互联网”，重点围绕基于真实 IPv6 源地址寻址的新一代可信任互联网体系结构及关键技术开展研究，建立大规模可信任互联网试验网；科技支撑计划项目“中国互动新媒体网络与新业务科技工程”，以广播影视业务为核心，建设相应的示范区，形成宽带、双向、多功能的互动新媒体网络。

科技部“973”计划支持了下一代互联网相关研究，主要包括 2003 年的“新一代互联网体系结构理论研究”及后续项目 2009 年的“新一代互联网体系结构和协议基础研究”、2007 年的“一体化可信网络与普适服务体系基础研究”等。

#### 5. 基础研究项目

国家自然科学基金委员会“十五”期间先后启动重大研究计划“网络和信息安全”和“以网络为基础的科学活动环境研究”，重点资助了下一代互联网体系结构、新一代网络应用平台和网络管理的基础理论和关键技术研究等项目。

#### 6. 电子信息产业发展基金项目

“十一五”期间，电子信息产业发展基金面向解决互联网发展中所面临的安全可信、可管可控等关键问题，支持了未来包交换网络的体系结构与关键技术研究、设备系统研发与网络实验等项目。

### 4.2.3　已建成全球最大的 IPv6 示范网络

通过实施 CNGI 工程，建成了大规模下一代互联网示范网络，包括 6 个主干网、2 个国际交换中心、273 个驻地网。其中，由中国教育和科研计算机网、中国电信、

中国联通、中国网通/中科院、中国移动、中国铁通承建了 6 个主干网。在北京和上海分别建成 CNGI 国际/国内互联中心，实现了 6 个主干网之间的互连，并连接了美国、欧洲、亚太地区的下一代互联网。在全国 100 所高校、100 个科研单位、73 个企业建成了 IPv6 驻地网。清华大学等 25 所高校建成的 CNGI－CERNET2 是目前世界上规模最大的纯 IPv6 互联网，取得了多项重大创新，总体上达到世界领先水平。

在此基础上，CNGI 示范网络提供了重大科研和新型业务的试验床。不仅为我国下一代互联网技术研究、标准制定、产品开发提供了科技创新和成果的测试平台，也为自然科学基金、“973”、“863”、“科技支撑”计划，以及中国科学院、教育部等单位组织的国家科研计划重大项目的实施提供了技术研发和开发试验环境。此外，各基础电信运营企业积极参与示范网建设，开展新型电信业务的应用试验和技术研究，取得了大量宝贵经验。

在长三角地区建设的“高性能宽带信息网 3TNet”，其骨干网具有 T 比特级的传输、交换和路由能力。该网络已在长三角地区进行了 3 万用户、为期一年的示范运行，并经历了 6 次专项试验和有数千人参与的大规模同步测试。后续将在长三角 15 个城市或地区开展 100 万用户规模的示范应用。

通过 CNGI 建设，相关企业、科研单位取得了大量示范性应用成果，部分已经在我国经济和社会建设中发挥了积极作用。例如，四川汶川特大地震灾害发生后，利用 CNGI 项目支持的中欧高速互连线路，把欧洲联合研究中心卫星观测的高分辨率的灾区遥感图片实时传送到中科院对地观测中心。北京奥运会期间，CNGI 北京互联中心开通 IPv6 奥运官网镜像站点，成为我国面向全球的 IPv6 重要应用示范，CNGI 项目支持开发的 IPv6 视频监控和传感器系统，成功应用于全国各地的 48 个体育场馆，圆满完成奥运通信保障任务，在国际上引起了很大反响。此外，“基于 IPv6 无线传感网络的环境监测系统”以开发淮河流域水资源污染监测系统为目标，为实现流域综合管理和灾害预警提供了先进的手段；“澜沧江-湄公河次区域资源环境安全区域合作中的应用示范”针对区域生态监测需要开发建立了试验平台。国内电信运营商建设的基于 IPv6 物联网的“湖南农业综合监控系统”获得了国际 IPv6 全球颁发的第一个 IPv6 Enabled ISP 认证证书。各大运营商响应国家号召，除了积极参加 CNGI 建设和试验工程项目外，还各自组织开展了大量卓有成效的下一代互联网发展推动工作，取得了一定成果，开展了农业信息化、智能家居、视频信息服务、家庭娱乐、统一消息和安全 VPN 等一系列应用试验。例如，我国运营商在 2009 年的两型社会实践和 2010 年上海世博会中提供了 IPv6 网络和相关应用服务；在 2011 年的深圳大运会上将进行 IPv6 网络搭建和业务运营。

### 4.2.4 初步形成较为完善的 IPv6 标准体系

我国的 IPv6 标准化工作在 2001 年全面启动，由中国通信标准化协会（CCSA）

具体负责，已经完成和正在制订的标准有 40 余项，初步形成较为完善的 IPv6 标准体系。国内 IPv6 标准的制订经历了三个阶段：第一阶段主要是国际标准本地化，完成了 IPv6 基本协议及路由协议等标准的制订；第二阶段是结合国内 IPv6 网络建设的需要，制订了一系列设备技术标准及测试标准；第三阶段是开始制订具有技术创新性的标准，目前在过渡技术标准方面取得了一定的突破。

在 CNGI 示范工程的带动下，近年来我国在国际互联网标准化工作方面取得了长足进展，在国际互联网标准化组织 IETF 中的主动权和话语权日益扩大。目前 IETF 有四个工作组由我国专家担当主席，分别是安全领域的 hokey、多连接领域的 mif、P2P 领域的 ppsp 和 decade。同时，我国专家还推动成立了 SAVI 和 Softwire 等工作组，并分别担任 SAVI 和 Softwire 工作组的技术顾问。我国在位置标识分离、移动性管理、物联网、多连接、安全、P2P、网络过渡、中文域名和中文邮件等领域发挥了重要作用。目前我国专家主导制定了 30 多项 IETF 标准，在一定程度上改变了我国长期以来在互联网核心技术方面受制于人的被动局面。

总体来看，我国 IPv6 标准整体上仍处于跟随国际标准的地位，IPv6 标准进展与国际标准基本一致，但在过渡类标准方面有所创新（如软线技术标准、IVI 技术标准等），已成为国际标准。目前，我国制定的一系列 IPv6 标准能够满足纯 IPv6 网络建设的需要，但是在 IPv4/IPv6 互通标准和应用类标准方面尚未完善，需要重点发展。

## 4.2.5　IPv6 产业得到长足发展

IPv6 相关产业主要涉及网络设备、业务设备、移动终端、应用软件、操作系统及芯片等。在 CNGI 示范网络建设中，坚持以国产设备为主，带动了国内的产业发展，加速了我国下一代互联网核心设备的产业化进程。目前 CNGI 示范网络的国产设备占到 50%以上。路由器、交换机、宽带接入设备、互联网关、音/视频监控摄像终端、无线传感器网络节点等产品已经批量投入市场，设备研发和产业化能力达到国际先进水平。在 IPv6 测试领域，中国团队积极参与全球测试规范的制订和实施，主导 IPv6 Enabled 测试认证工作，中国专家担任测试工作组主席，目前在中国团队主导下，全球已有 60 家 ISP 和 494 家网站通过了 IPv6 Enabled 认证。总体而言，我国 IPv6 产业优势主要集中在网络设备和业务设备，而在操作系统[①]和芯片[②]等环节相对薄弱，存在短板。

就网络设备而言，产品类型基本上已覆盖原有 IPv4 产品（包括路由器、交换机、宽带接入服务器等），而且基本与国际同步，并在 CNGI 示范网络中得到实际部署验证。但是，IPv4/IPv6 网络互通类设备（如 CGN）与商用规模部署的电信级要求还有

① 操作系统包括 PC 操作系统和手机操作系统。

② 芯片包括手机芯片、网络设备芯片等。

一定的距离。业务网络设备主要集中在 SIP 服务器、综合接入设备、企业网关及家庭网关等边缘设备；传统核心网设备，如软交换、中继媒体网关、信令网关、IMS 系统、基站控制器、3G 分组域子系统及智能网系统等 IPv6 支持能力比较弱。各厂商虽然目前尚未推出大容量 IPv6 核心网设备，但均已在数据网络产品中完成了相关技术研究积累，且部分核心网设备在信令层面已经支持 IPv6，一旦 IPv6 核心网设备市场需求出现，各厂商可在短期内推出相应的 IPv6 产品。

在信息家电领域，我国企业（如海尔、康佳、海信等）已开始涉足 IPv6 终端产品的研发，但目前来看支持 IPv6 的产品类型还比较少。在移动智能终端领域，由于手机芯片和操作系统基本上由国外厂商垄断，所以对 IPv6 的支持能力基本与国际同步，目前还没有一款支持 IPv4/IPv6 的双栈商用手机。

在操作系统方面，基本由国外软件厂商所垄断。目前 PC 操作系统（包括 Linux、UNIX、Windows 等）都支持 IPv6 的版本，但客户端需要配置启用；手机操作系统（包括 Android、ioS、RIM、Symbian、Windows Mobile 等）主流厂商都宣称能够提供支持 IPv6 的版本，但多数终端预装版本并不支持 IPv4/IPv6 双栈。

在应用软件方面，总体而言，开发进度远远落后于操作系统。目前绝大多数基于 Windows 平台的应用软件都不支持 IPv6，如 QQ、迅雷及一些游戏客户端软件等，但通用浏览器可以支持 IPv6。

在芯片方面，国内厂商主要在 TD 芯片（如展讯）和 WCDMA 芯片（如海思、联发科）上有所突破，但目前支持 IPv6 的型号还比较少[①]。

## 4.2.6 IPv6 发展面临的主要问题

目前，我国 IPv6 发展主要存在以下几方面的问题。

### 1. IPv6 全面商用部署缺乏核心驱动力

IPv6 部署的根本动因来自于 IPv4 地址资源不足，并不能解决现有互联网所面临的各种问题（如服务质量、安全等），也缺乏有效的商业模式创造经济效益，但又需要大量资金投入，因此产业链各方商业动机不足，而单靠某个环节行动又无法真正启动 IPv6 商用部署，因此导致我国 IPv6 部署出现中间强（网络）、两端弱（终端和应用）的格局。

### 2. 运营商网络各环节 IPv6 支持状况不一，向下一代互联网过渡的准备不足

运营商网络 IPv6 的支持情况可以分为两部分：一部分是网络自身，包括接入网、城域网和骨干网对 IPv6 的支持情况；另一部分是后台业务支撑系统，包括计费系统、

① 根据前期调研，目前 TD 芯片 PXA920 可以支持 IPv6 单栈，LTE 芯片 PXA1802 可以支持 IPv4/IPv6 双栈。

网管系统、域名系统及认证鉴权系统等对 IPv6 的支持情况。

从网络部分来看：① 骨干网，路由器设备对 IPv6 的支持情况较好，多数硬件没有问题，只需要对软件进行升级。② 城域网，多数 BRAS（宽带网络接入服务器）和 SR（业务路由器）硬件问题不大，但是大部分软件需要升级，特别是很多 BRAS 软件尚不支持 PPPoE for IPv6 功能。移动分组域 GGSN/PDSN 硬件没有问题，但是需要进行软件升级。③ 接入网，传输和交换系统可以作为纯二层处理，将三层功能放在 BRAS 或 SR 网关处理，因此在 IPv6 业务部署初期其是否支持 IPv6 对业务的影响不大。而路由型家庭网关目前基本都不支持 IPv6，需要进行升级替换。

从后台业务支撑系统来看，整体上对 IPv6 的支持还比较弱，需要对整个系统进行较大规模的改造，包括计费系统、网管系统、认证鉴权系统及域名系统等。

三个国内网络运营商都建有 CNGI 商业试验网，开展了 IPv6 业务试验和示范应用，但是整体来看运营商还没有完备的过渡方案来有效解决 IPv4/IPv6 互通问题。

### 3. 网络过渡类产品还无法满足电信级商用部署的需求

IPv6 网络商用部署必须解决两个关键问题：一个是 IPv4 和 IPv6 网络共存；另一个是 IPv4 和 IPv6 业务互通。目前，就上述问题 IETF 相关工作组已经开发了三大类过渡技术方案，包括双栈、隧道和翻译，其中双栈和隧道用于解决网络共存问题，技术比较成熟；翻译用于解决 IPv4 与 IPv6 业务互通问题，技术尚未成熟。目前还没有一种机制能够完全解决 IPv4 与 IPv6 网络共存和业务互通问题，在网络过渡时期需要根据实际应用场景综合应用多种机制，增加了网络部署的复杂度。

当前，运营商解决 IPv4/IPv6 网络共存的过渡方案已基本明确，即私网双栈（NAT444）和轻量级隧道（DS_Lite）两种。其中 NAT444 沿用现有 NAT 技术，通过引入大容量电信级 NAT 设备（CGN）实现 IPv4 私网地址的两级翻译[①]，同时利用 NAT444+IPv6 方式形成私网双栈架构，实现向 IPv6 的过渡。DS-Lite 在现有 NAT 技术基础上，引入 IPv4-in-IPv6 隧道，形成 NAT+隧道+IPv6 架构实现过渡。DS-lite 的核心是通过使用 IPv6 隧道来避免两次穿越 NAT 带来的复杂性，不需要为用户规划和管理私网地址。从设备层面看，两种过渡技术设备都有主流厂家支持，但是设备距离商用规模部署的电信级要求还有一定的距离。

为解决 IPv4 和 IPv6 业务互通，目前只有翻译技术，典型技术有 NAT64 和 IVI。其中 NAT64 是一种从 IPv6 到 IPv4 的转换技术，主要考虑过渡初期 IPv6 终端对 IPv4 资源的访问，不涉及 IPv4 访问 IPv6 资源的情况。IVI 技术采用无状态的 IPv4/IPv6 地址映射和无状态协议翻译机制，实现了 IPv4 和 IPv6 的双向互访，但是 IVI 不解决

① 第一级是用户 IPv4 私网地址到运营商 IPv4 私网地址的翻译；第二级是运营商 IPv4 私网地址到 IPv4 公网地址的翻译。

IPv4 的地址紧缺问题[①]。从设备层面看，这两类技术还不成熟，特别是在满足电信级应用的性能和可靠性需求方面还有待进一步完善。

#### 4. 信息监管面临挑战，安全技术及产品有待进一步完善

与 IPv4 协议相比，IPv6 仅扩充了地址空间和简化了 IP 报头，并没有从根本上改变 IP 体系结构，因此 IPv6 面临的安全风险和 IPv4 没有本质区别，许多 IPv4 中的安全问题在 IPv6 中同样存在，如窃听攻击、应用层攻击、中间人攻击、洪泛攻击等。此外，由于 IPv6 协议栈集成了 IPsec 协议，为终端应用提供了更为便捷的端到端加密方式。

IPv6 地址空间的扩大和 IPsec 加密的使用，使得国家网络与信息安全防护体系面临极大的挑战：IP 黑白名单监管规则数量爆炸式增长；使用 IPsec 加密通信时，除通信双方外中间环节无法获知内容，将会导致目前建立在内容识别基础上的安全技术手段失效或能力下降；网络与信息安全事件的事后追溯能力急需加强。此外，IPv6 技术还没有在现网上大规模部署，很多协议漏洞和潜在的安全风险还没有充分暴露，需要进一步的研究。网络安全类产品，包括防火墙、安全网关、内容过滤、入侵检测等设备还需要开发以支持 IPv6。

## 4.3 我国 IPv6 过渡方案

目前 IPv6 协议族日趋完善，IPv6 网元设备也逐步增多，在此基础上可以组建纯 IPv6 网络。但是在实际应用环境中，需要考虑在 IPv4 网络如何引入 IPv6 的问题。

研究 IPv4/v6 综合组网技术涉及许多内容，这包括网络的各个层面，如网络结构、功能集合、网络路由、域名体系、地址分配、服务质量、典型应用、管理功能与接口、安全要求等方面。

概括地讲，IPv4/v6 综合组网技术的主要研究包括以下内容。

#### 1. 现有不同过渡策略与网络过渡工具的技术特点及其适用范围

经过 IETF 的“下一代网络过渡技术工作组（NGTRANS）”对 IPv4 网络向 IPv6 网络过渡技术的多年研究，已经提出了许多网络过渡策略（如双栈策略、隧道策略、翻译策略等）和相应的过渡工具（不同的策略均有多个对应的过渡工具），这些策略和工具分别有着自己的适用环境和应用条件，相应地也有着不同的应用效果。对这些策略和工具进行综合比较和对比分析能够进一步明确它们的适用范围和技术特点，从而确定它们在网络中的地位和应用环境。

① 目前提出了 dIVI 的解决方案，可以通过端口来实现 IPv4 公网地址的复用。

### 2. IP 承载网络中引入 IPv6 后的网络结构

在传输网络和业务网络之间是 IP 承载网络，它可以进一步分为两个层次：IP 传输子层和 IP 承载控制子层。当在 IP 传输子层中引入 IPv6 技术以后，使得 IP 承载网络的网络结构和网络逻辑结构发生了变化，这些变化不但会影响业务层，而且对底层传输网络也会产生一定的影响。通过对引入了 IPv6 之后的 IP 承载网络的网络结构进行分析，可以进一步明确基于 IP 的运营网络中，各个网络层次的功能及其相关层次。这对于分析网络的互联互通、业务的提供方式均有重要意义。

### 3. 电信网络的不同网络环境对 IPv4/v6 综合组网提出的技术需求

IP 技术在电信网络中的应用范围越来越广，电信网络和互联网络在设计理念、网络结构、运维模式、业务提供方式等方面均有着重大差别。IETF 的“IPv6 网络互操作工作组（IPv6OPS）”正在研究的典型网络环境需求是针对互联网的，虽然其研究成果会对电信网络的典型网络环境的需求分析有一定的参考价值，但是也有一定的局限性。因此需要对电信网络的不同典型网络环境的研究有足够的重视，不同的网络环境会对 IPv4/v6 综合组网技术提出不同的要求。这些典型的网络环境包括：骨干网络、城域网（包括接入、汇聚、核心等层次）、驻地网等部分。

### 4. 针对不同的网络环境（不同的需求）提出可能的综合组网方案

针对不同的典型网络环境提出可能的综合组网方案，并对这些组网方案的技术特点、应用范围、应用效果、局限性等方面进行分析。这些组网方案即将成为电信网络组网方案的选择对象；这些组网方案的比较分析结果将成为电信网络组网方案的选择依据。

### 5. IPv4/v6 综合组网时的路由问题

在 IPv4/IPv6 综合组网技术中，路由问题是一个需要着重分析的关键问题。这个问题包括如下几个方面：路由方式的选择、路由可达性分析、路由泄漏问题、路由环回问题、路由聚合问题及不同过渡策略综合应用时的路由可达问题等。

其中路由泄漏是指 IPv4 网络与 IPv6 网络的路由相互泄漏，从而使得不同路由策略域（自治域）内的路由数目膨胀，路由管理复杂，路由效率下降，还可能产生路由环回现象。

为了提高网络路由效率、减少网络路由表的大小，一种可能的方法是对路由进行聚合，这一点在 IPv4 路由策略的研究中已经受到了重视，由于 IPv6 的地址数目较多，路由聚合功能成为 IPv6 路由策略所必需的功能，因此在 IPv6 协议的设计之初就给予了足够的重视。在 IPv4/v6 综合组网环境中，使得路由聚合问题变得更为复

杂，需要进行深入的分析。

### 6. IPv4/v6 综合组网时的域名问题

域名解析/反向解析 DNS 既是 IP 网络中的一种业务，也是 IP 网络的一种基础功能。在许多信息检索业务中，均需要 DNS 功能。在 IPv4/v6 综合组网环境中，应该考虑的有关域名的问题有如下两方面：① 需考虑 IPv6 地址相关域名的标识与解析方法，这方面的研究在 IETF 的 RFC 中已经进行了规定；② 需考虑域名空间连通性问题，这也是技术上，尤其是工程上较难解决的问题。

DNS 服务器支持的 IP 协议的不同可能引起域名空间的分裂，一些 DNS 服务器可能不能按照同一 IP 协议从根服务器可达，从而造成有些域名不能获得解析。

解决这个问题可以有多种思路：① 可以要求综合组网环境中的所有 DNS 服务器均支持 IP 双栈协议；② 可以采用 DNS 代理服务器（其为双栈服务器），由其来代理一些 DNS 查询，从而使得支持 IPv4 地址的 DNS 空间与支持 IPv6 地址的 DNS 空间可以互通；③ 可以制订相应的 DNS 管理策略，保证某一个 DNS 区域内至少有一个 DNS 服务器是同时 IPv4/v6 可达的。尽管有上述可以采用的策略，但是在实际组网中依然会遇到许多问题，如现在主机操作系统甚少支持以 IPv6 包的形式来发送 DNS 消息，这为网络设计带来了一定的难度。

### 7. IPv4/v6 综合组网时的安全性分析

IPv4 网络的安全性一直受到批评，为此在 IPv6 协议的设计过程中考虑了网络安全的需求，在 IPv6 的包头中设计了安全包头，它可以基于 AH 或 ESP 进行通信，从而在一定程度上提高了网络的安全性。但是在综合组网环境中，这个问题变得更为复杂。一方面，在综合组网环境中 IPv6 的安全特性由于 IPv4 的存在而不能充分发挥；另一方面，隧道技术在综合组网环境中的应用也增加了网络的新的潜在不安全因素。还有，各种综合组网技术均需要进行相应的安全性分析。另外，IP 承载层的安全性只是网络（包括业务层、业务控制层、承载层、支撑层等多个层面）安全性的一个方面，当从整网的角度来分析承载层的安全性时，增加了问题的复杂程度。

### 8. IPv4/v6 综合组网时的地址分配策略

IPv6 的地址分配策略由 IETF 相关的 RFC 进行规定（最近 IETF 的地址分配的建议有了新的进展，如新颁布了 RFC 3177，同时 RFC 3587 取代了原来的 RFC 2374、RFC 3513 取代了 RFC 2373），同时具体的地址分配方法由相关的互联网管理组织进行。这里所要讨论的是一个运营商在拿到地址时如何在自己的网络中进行分配、在地址分配时所应依据的原则，以及与具体组网技术相关的地址需求分析等。

9. 不同组网技术在网络中的互联互通性（相容性）

目前，存在的多种 IPv4/v6 综合组网技术在网络中综合应用时可能会产生一些问题，如利用这些技术组建的网络之间的互联互通性就是一个需要主要考虑的问题。有时，利用一种组网技术组建的网络不能与用其他组网技术组建的网络进行相互通信，这包括地址类型的问题、路由的问题、域名的问题、协议翻译的问题等多个方面，因此需要仔细分析，作为评价和选择 IPv4/v6 综合组网技术的一个重要依据。

## 4.3.1　网络演进的基本原则

运营商网络向 IPv6 演进是一个长期的系统工程，涉及用户终端、接入网、城域网、核心网、信源及业务支撑系统等多个方面，为实现网络的平滑演进，既要考虑现网 IPv4 设备的投资保护，又要尽量减少对用户和应用的影响，因此必须遵循以下基本原则。

1. 业务驱动

下一代互联网演进的主要驱动力来自于业务，一方面需要保证现有业务的发展不受 IPv4 地址的局限，另一方面也要支持未来新兴业务（如移动互联网、云计算、物联网及三网融合等业务）的发展需求。

2. 过渡平稳

保证过渡阶段现有网络稳定运行，IPv4 的用户和业务体验尽量不受影响。过渡技术和组网方案应减少对网络架构和系统架构的影响，确保过渡期的平稳性。

3. 技术创新

在过渡的不同阶段会面临不同的场景和需求，应关注技术创新和新技术的部署实施，逐步引入 IPv6 新业务，丰富 IPv6 网络流量，提升用户体验。

4. 成本兼顾

过渡方案在满足业务需求和网络演进的基础上，应尽可能兼顾网络部署的难度和成本，降低网络部署的复杂度，必须能够采用渐进式部署的方式，确保可持续发展。

而在制定具体方案时，还需要充分考虑 IPv4 与 IPv6 协议不兼容带来的问题，需要构建相关的过渡机制来支持二者无缝地并存，应遵循以下必要原则：

① 保证 IPv4 和 IPv6 主机之间的互通，在 IPv4 业务和 IPv6 业务互不影响的前提下支持 IPv4 业务与 IPv6 业务的互通；

② 保证现有 IPv4 应用在综合组网环境中的正常应用；

③ 避免设备之间的依赖性，设备的更新须具有独立性；

④ 综合组网过程对于网络管理者和终端用户来讲要易于理解和实现；

⑤ 提高组网灵活性，支持网络的渐进性升级，用户拥有选择何时过渡和如何过渡的权利；

⑥ 综合组网以后网络的服务质量不应该有明显的影响；

⑦ 综合组网以后网络的可靠性和稳定性不能削弱；

⑧ 综合组网以后网络管理功能应该比原有网络有所加强；

⑨ 在设计综合组网方案时，要考虑 IPv4/v6 长期共存的事实，也要考虑将来网络平滑过渡的问题。

## 4.3.2 网络演进的过渡场景

### 1. 运营商网络架构

目前我国三大运营商的网络架构都在向扁平化的趋势发展，其典型架构如图 4-3 所示，从用户终端到应用服务提供商经由接入网（包括有线接入、无线接入）、城域网和骨干网。

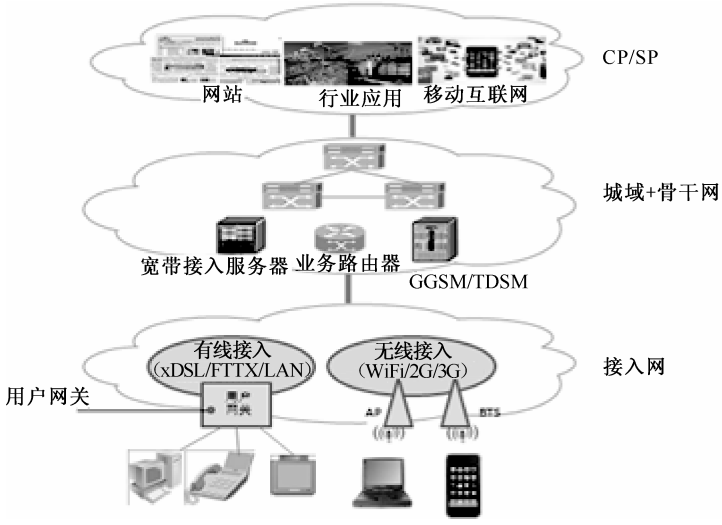



图 4-3 运营商典型网络架构

### 2. 过渡场景

运营商网络升级改造的过渡场景可以从用户、网络和业务提供商三个维度进行

分析。

（1）用户

固网用户根据接入网络环境的不同可以分为两大类：一类通过二层桥接设备（如ADSL、FTTx）接入运营商网络，另一类通过三层路由设备（如具有路由功能的 CPE 网关）接入运营商网络。对于前者，用户的 IPv6 支持能力主要取决于终端操作系统（既要支持 IPv6 协议栈，又要能为上层应用提供 IPv6 的编程接口），而对于后者，用户的 IPv6 支持能力不但取决于终端操作系统而且取决于 CPE 设备的双栈能力。在过渡阶段，用户终端通过网络获取 IP 地址的形态包括以下几种类型。

① 仅获得 IPv4 地址（终端操作系统不支持 IPv6）；

② 获得 IPv4 公网地址和 IPv6 地址；

③ 获得 IPv4 私网地址和 IPv6 地址；

④ 仅获得 IPv6 地址（如封闭的物联网应用终端）。

对应的应用类型可以分为仅支持 IPv4 的应用、支持 IPv4/IPv6 双栈应用和仅支持 IPv6 的应用。

（2）网络

网络的演进是一个循序渐进的过程，在过渡阶段会并存多种形态的网络，包括 IPv4 单栈网络、IPv4/IPv6 双栈网络和 IPv6 单栈网络。目前，城域网和骨干网的演进技术路线较为明确，IP 网络采用双栈，MPLS 网络采用 6PE 技术路线。经过多年的网络扩容和设备更新换代，城域网和骨干网大部分设备能够支持 IPv4/IPv6 双栈。而对于接入网，由于接入技术类型多样（如 ADSL、以太网、FTTx、WLAN 等），设备能力参差不齐，所以是整个网络升级改造的难点和重点。

对于二层接入网，针对一些特定的应用（如组播），要求网络设备具备三层报文的侦听能力；而对于三层接入网，需要结合网络平滑演进的整体规划，以双栈技术为基础，辅以隧道技术进行网络的部署。

（3）业务提供商

互联网业务应用的升级改造也应是循序渐进的过程，要求用户无感知并且不会对用户的业务体验带来较大的负面影响。在过渡阶段，应用将会出现三种形态：仅支持 IPv4 的应用、支持 IPv6 的应用及支持 IPv4/IPv6 的应用。要保证 IPv4 用户无影响地访问原有 IPv4 业务，也要保证 IPv6 用户能够访问已有的 IPv4 业务，而且保证 IPv4 用户能够访问 IPv6 新业务。

### 3. 典型场景分析

网络由 IPv4 向 IPv6 过渡将是一个长期的演进过程，在过渡期主要存在以下两

种通信模型。

（1）同种协议间的通信

同种协议间的通信是指通信双方的协议类型是一致的（如 IPv4 用户访问 IPv4 业务，IPv6 用户访问 IPv6 业务），其间可以通过隧道技术穿越不同协议类型的网络（如 4-6-4、6-4-6），也可以穿越同种协议类型的网络（如 4-4-4、6-6-6）。

（2）异种协议间的通信

异种协议间的通信是指通信双方的协议类型是不一致的（如 IPv4 用户访问 IPv6 业务、IPv6 用户访问 IPv4 业务），主要解决 IPv4 和 IPv6 应用之间的互访问题。

表 4-1　IPv4 向 IPv6 过渡的场景描述

| 通信模型 | 用户 | 网络 | | | 业务 | 应用场景 | 描述 |
|---|---|---|---|---|---|---|---|
| | | 接入网 | 城域网（POP 点以上） | 骨干 | | | |
| 同种协议同构网络 | IPv4 | IPv4 | 双栈 | 双栈 或 6PE/6VPE | IPv4 | 4-4-4 | IPv4 用户通过 IPv4 网络访问 IPv4 业务 |
| | IPv6 | IPv6 | 双栈 | 双栈 或 6PE/6VPE | IPv6 | 6-6-6 | IPv6 用户通过 IPv6 网络访问 IPv6 业务 |
| 同种协议异构网络 | IPv4 | IPv6 | 双栈 | 双栈 或 6PE/6VPE | IPv4 | 4-6-4 | IPv4 用户通过 IPv6 网络访问 IPv4 业务 |
| | IPv6 | IPv4 | 双栈 | 双栈 或 6PE/6VPE | IPv6 | 6-4-6 | IPv6 用户通过 IPv4 网络访问 IPv6 业务 |
| 异种协议同构网络 | IPv4 | IPv4 | 双栈 | 双栈 或 6PE/6VPE | IPv6 | 4-4-6 | IPv4 用户通过 IPv4 网络访问 IPv6 业务 |
| | IPv6 | IPv6 | 双栈 | 双栈 或 6PE/6VPE | IPv4 | 6-6-4 | IPv6 用户通过 IPv4 网络访问 IPv4 业务 |
| 异种协议异构网络 | IPv4 | IPv6 | 双栈 | 双栈 或 6PE/6VPE | IPv6 | 4-6-6 | IPv4 用户通过 IPv6 网络访问 IPv6 业务 |
| | IPv6 | IPv4 | 双栈 | 双栈 或 6PE/6VPE | IPv4 | 6-4-4 | IPv6 用户通过 IPv4 网络访问 IPv4 业务 |

## 4.3.3　网络演进过渡技术方案

### 1. 总体架构

运营商网络可以简单地划分为接入网、城域网和骨干网，其中接入网又分为桥接型的接入网和路由型的接入网。对于网络的演进，可以采用双栈、隧道和翻译相

结合的技术方案。接入网在演进的过程中，可能会出现三种场景，即 IPv4 接入网、IPv6 接入网和 IPv4/IPv6 双栈接入网，可以考虑采用 6over4 或 4over6 的技术方案，隧道的两个端点分别在用户侧家庭网关（或者终端，通过加载软件插件）和网络侧设备上（如 CGN、网关）。对于骨干网和城域网，如果是 IP 承载，采用双栈方案；如果是 MPLS 承载，采用 6PE 方案。

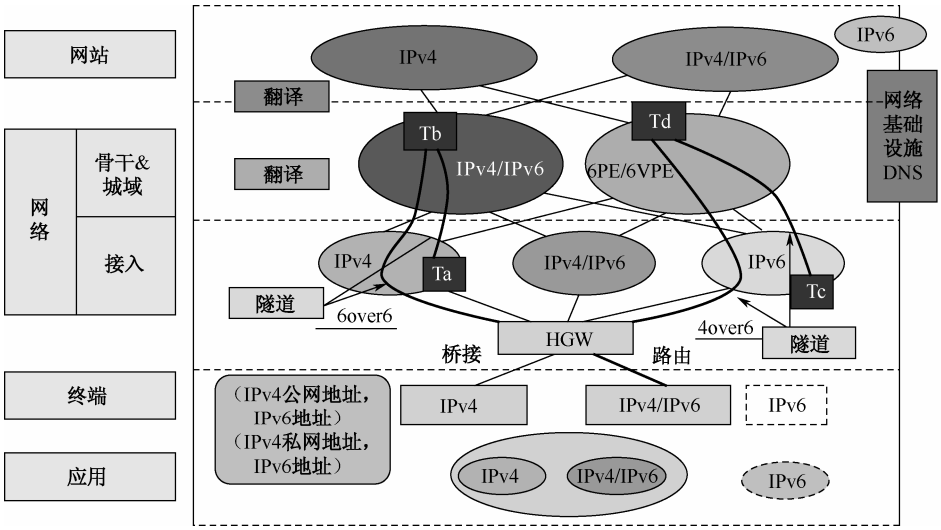



图 4-4　向 IPv6 演进的总体技术方案

### 2. 骨干网

（1）基于 IP 技术

在 Native IP 骨干网络中部署 IPv6 最成熟的方案就是采用双栈技术，该方案要求对现网设备进行双栈升级改造。

（2）基于 MPLS 技术

在 MPLS 骨干网络中部署 IPv6，最简单的方式是先维持 P（核心）路由器 IPv4 单栈，在网络边缘 PE 路由器上实现双栈，把 IPv6 流量承载到基于 IPv4 的 MPLS 标记路径上传输。

（3）技术特点

① 在 IPv4 网络中，PE 和 P 路由器之间仍然使用 IPv4 的 IGP 协议（如 IS-IS）来建立相互之间的路由关系，也仍然使用 IPv4 的标签分发协议（如 LDP、RSVP-TE 等）来建立 PE 与 PE 之间的 LSP（标记交换路径）。因此，对 P 路由器和 PE 路由器

来说，IPv6 网络是不可见的。

② 需要使用 MP-BGP 多协议扩展属性为 IPv6 网络传播路由信息。

③ 6PE 路由器或 6VPE 路由器都不是一个专用的设备，其在为 IPv6 网络提供隧道服务或 VPN 服务的同时也可以在其他接口或子接口上为普通的 IPv4 用户提供 MPLS VPN 业务。

（4）实施方案

在 MPLS 骨干网上提供 IPv6 的服务可以采用以下方式。

① 在 MPLS 骨干网的边缘 PE 路由器上部署 IPv6，在现有 IPv4 互联网接入的边界路由器上提供 IPv6 互联网接入。

② 在 VPN 和互联网接入业务中，使用 IPv4 的标签交换路径（LSP）承载 IPv6。通过采用 6PE 或 6VPE，可避免在网络核心 P 路由器上对现有网络的网络配置进行任何形式的修改，如既有的 IGP 协议、标签分发协议 LDP、现有的地址编址等。

③ 在部署过程中需要特别注意 ICMPv6 和 IPv6 MTU 的问题。由于网络核心的 P 路由器不支持 IPv6，将会丢弃 ICMPv6 报文，因此路径 MTU 发现机制必须在网络边缘来实现。

### 3. 城域网+接入网

城域网主要由三层路由设备（CR，核心路由器）和业务控制设备（SR，业务路由器，BRAS，宽带接入服务器）组成，主要实现 IP 报文的转发和业务分流；接入网主要由二层接入设备（DSLAM、交换机、OLT/ONU 等）组成，主要实现 IP 报文的接入。

表 4-2　Native IPv6 和 6PE/6VPE 比较

| | Native IPv6 | 6PE/6VPE |
|---|---|---|
| 实施成本 | 所有设备升级支持 IPv6，实施成本高 | PE 设备升级支持 IPv6，P 设备不需要升级，实施成本低 |
| 协议部署 | 所有路由器运行 IPv6 IGP/BGP | MPLS 核心不变，PE 之间部署 MP-BGP |
| 可扩展性 | 没有限制 | 没有限制 |
| 维护成本 | 需要所有节点维护新引入的 IPv6 协议和路由 | IPv6 作为 MPLS 新业务，对现有网络维护冲击小，维护范围限制在 PE |
| 业务支持 | 单播/组播 | 组播不成熟，可支持 VPN 业务 |

对于城域网，在 POP 点之上应采用双栈技术路线，并根据需要部署相应的网关设备终结隧道并完成协议转换；接入网过渡技术方案应以双栈技术为基础，结合隧道和翻译机制，根据不同的应用场景采用不同的过渡方案。

① 内容和应用没有明显变化，运营商趋向 CGN 技术，采用私网双栈+NAT444；

② 内容和应用没有明显变化，运营商趋向 IPv6，采用 DS-Lite 提供私网 IPv4 用户的接入，部署 NAT44 实现私网 IPv4 到公网 IPv4 的转换；

③ 多数内容和应用转向双栈，采用双栈；

④ 用户转向单栈 IPv6，采用 6rd 提供 IPv6 用户的接入，NAT64/IVI 翻译机制实现 IPv6 用户访问 IPv4 网络的业务资源；

⑤ 多数内容和应用转向 IPv6，采用 DS-Lite 提供公网 IPv4 用户的接入，IVI 翻译机制实现 IPv4 用户访问 IPv6 网络的业务资源。

对于大二层接入网络，接入设备对转发的报文透明传递，但是应能够识别、区分 IPv6 报文和 IPv4 报文，并能够根据 IPv6 协议部分进行 VLAN 标记、QoS、报文过滤等处理操作。如果支持双栈，可以直接通过数据链路层协议承载 IPv6 协议（如 PPPoE 和 IPoE）。

表 4-3　过渡场景对应的演进技术方案

| 通信模型 | 用户 | 网络 | | | 业务 | 应用场景 | 演进技术方案 |
|---|---|---|---|---|---|---|---|
| | | 接入网 | 城域网（POP 点以上） | 骨干 | | | |
| 同种协议同构网络 | IPv4 | IPv4 | 双栈 | 双栈 或 6PE/6VPE | IPv4 | 4-4-4 | 私网双栈+NAT444 |
| | IPv6 | IPv6 | 双栈 | 双栈 或 6PE/6VPE | IPv6 | 6-6-6 | |
| 同种协议异构网络 | IPv4 | IPv6 | 双栈 | 双栈 或 6PE/6VPE | IPv4 | 4-6-4 | DS-Lite 方案 |
| | IPv6 | IPv4 | 双栈 | 双栈 或 6PE/6VPE | IPv6 | 6-4-6 | 6rd 方案 |
| 异种协议同构网络 | IPv4 | IPv4 | 双栈 | 双栈 或 6PE/6VPE | IPv6 | 4-4-6 | 远期 IPv6 网络及应用成为主流时才会出现该场景 |
| | IPv6 | IPv6 | 双栈 | 双栈 或 6PE/6VPE | IPv4 | 6-6-4 | NAT64/IVI |
| 异种协议异构网络 | IPv4 | IPv6 | 双栈 | 双栈 或 6PE/6VPE | IPv6 | 4-6-6 | 远期 IPv6 网络及应用成为主流时才会出现该场景 |
| | IPv6 | IPv4 | 双栈 | 双栈 或 6PE/6VPE | IPv4 | 6-4-4 | 6rd + NAT64/IVI |

说明：

① 私网双栈+NAT444 方案：对于桥接型接入网，仅要求升级局端设备（如 BRAS、OLT）支持双栈，能够为终端同时分配 IPv4 和 IPv6 地址；如果是路由型接

入网，需要同时升级用户家庭网关设备和局端设备（如 BRAS、OLT）支持双栈，并且要求能够支持 NAT44 功能，而且要对用户侧私网地址空间和运营商接入网侧私网地址空间进行规划，避免冲突。用户终端能够获得 IPv4 私网地址和 IPv6 地址。

② DS-Lite 方案：适用于路由型接入网（不考虑用户终端通过安装插件实现客户端功能的情况），要求升级用户家庭网关设备支持双栈和 B4 功能；局端设备支持双栈、AFTR 功能以及 NAT44 翻译功能。用户终端获得 IPv4 私网地址和 IPv6 地址。

③ 6rd 方案：适用于路由型接入网（不考虑用户终端通过安装插件实现客户端功能的情况），要求升级用户家庭网关设备支持双栈和 6rd 客户端功能；局端设备支持双栈和 6rd 网关功能。用户终端获得 IPv6 地址，用户家庭网关分配 IPv4 公网地址。

④ NAT64 有状态互通方案：主要实现 IPv6 用户访问 IPv4 业务（有状态），可以根据需要在 IDC 出口或城域网内部署 NAT64 翻译设备，同时相应地部署 DNS64 设备。

⑤ IVI 无状态互通方案：实现 IPv6 用户访问 IPv4 业务或 IPv4 用户访问 IPv6 业务（无状态），可以根据需要在 IDC 出口或城域网内部署 IVI 翻译设备，同时需要对 DNS 域名系统进行升级改造。

### 4. 域名系统

在 IPv4 到 IPv6 的过渡过程中，由于 IPv4 和 IPv6 的 DNS 记录格式等方面有所不同，因此作为 Internet 基础架构的 DNS 服务需要进行升级和改造。目前，可以考虑采用两种不同的演进技术方案：一种是升级成双栈；另一种是基于翻译机制。

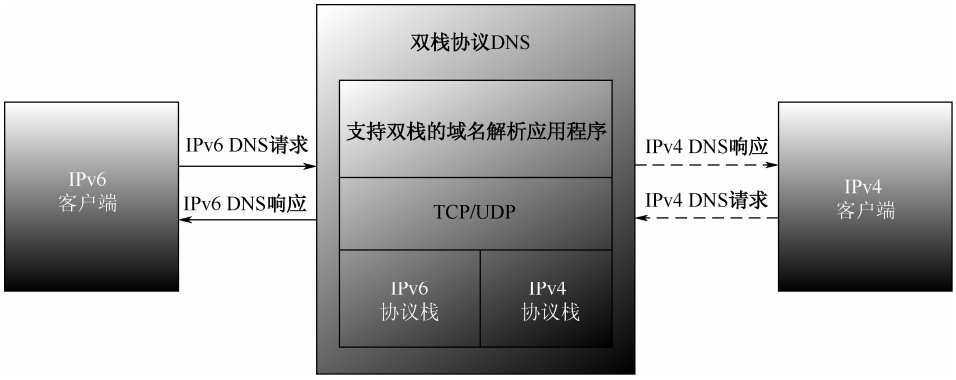



图 4-5　双栈网络+双栈 DNS 模型

将 DNS 升级支持双栈，IPv6 用户的访问返回“AAAA”记录，IPv4 用户的访问返回“A”记录。

另外一种方案是采用翻译机制，即 DNS64 技术。通常 NAT64 和 DNS64 是协同工作的，其应用场景是 6-6-4，基本原理是：当 IPv6 only 的用户访问 IPv4 单协议栈的服务器时，服务器的 IPv4 地址将经 DNS64 服务器进行前缀合成（特定地址前缀，

64:FF9B::/96），该特定前缀网段的流量将被路由转发至 NAT64 路由器上，从而实现 IPv6 与 IPv4 地址和协议的转换。

DNS64 则主要配合 NAT64 工作，主要是将 DNS 查询信息中的 A 记录（IPv4 地址）合成到 AAAA 记录（IPv6 地址）中，返回合成的 AAAA 记录用户给 IPv6 侧用户（参见图 4-5）。

### 5. 典型过渡方案

由于互联网应用场景多种多样，因此 IPv6 演进技术方案没有统一的模式。对于运营商来说，IPv6 是未来针对 IPv4 地址短缺问题的根本解决方案，也是一个逐步演进的过程，选择过渡技术要综合考虑以下因素：保护现网投资，成本合理，网络改造难度适中，现有业务不受损，用户体验好。不同 IPv6 演进技术的采用和选择关键往往不仅是一个纯粹的技术思考，其更大的挑战是互联网发展与技术转型对运营和商业模式的影响。所以，应结合不同的业务应用场景和网络未来发展需求，综合考虑各种因素，结合多种过渡技术制定网络平滑演进的策略。

目前，网络演进的技术方案主要聚焦于以下几种，分别是私网双栈+NAT444，DS-Lite+NAT44、6rd 及 IPv6 与 IPv4 互通方案 NAT64/DNS64 和 IVI。

（1）方案一：私网双栈+NAT444

NAT444 就是两级 NAT，用户侧 HG（家庭网关）一级 NAT44，运营商一级 NAT44（LSN 设备），完成两级地址转换，形成三块地址空间，即用户侧私有地址、运营商私有地址、公网地址。该方案要求用户终端和家庭网关均支持双栈，并且均分配一个私网 IPv4 地址（不同的地址空间）和一个 IPv6 地址。IPv6 的业务流量按照 Native IPv6 进行转发，IPv4 的流量需要进行两级 NAT 转换，在运营商 CGN 设备翻译成公网 IPv4 地址，具体如图 4-6 所示。

NAT444 方案可以提高 IPv4 地址的复用率，缓解地址枯竭问题，而且便于部署，只需升级用户家庭网关支持双栈、网络侧在汇聚层或核心层增加 CGN 设备即可。从用户感知度、技术成熟度和部署难易度等方面考虑，NAT444 是目前比较好的方案。但是采用这种方案会增加 P2P 类业务实现难度，无法实现端到端的透明性，同时增加地址溯源的难度。

（2）方案二：DS-Lite+NAT44

DS-Lite 是 IPv6+4over6 隧道的典型方案。在城域网络中部署 DS-Lite CGN 设备，宽带接入服务器到核心路由器通过 IPv6 连接，用户的 CPE 支持 DS-Lite，CPE 到 DS-Lite CGN 之间建立 IPv4 over IPv6 隧道。宽带接入服务器给用户 CPE 分配 IPv6 地址前缀，用户主机的 IPv4 地址由 CPE 分配 IPv4 私有地址。用户的 IPv6 流量通过宽带接入服务器直接上行到核心路由器，用户的 IPv4 流量到 CPE 后，经过 IPv4 over

IPv6 隧道上行到 DS-Lite CGN 上，CGN 同时具有 NAT44 的功能，用户的 IPv4 数据经隧道解封装后，再做一次 NAT44 地址转换，最终发送到 IPv4 骨干网，具体如图 4-7 所示。

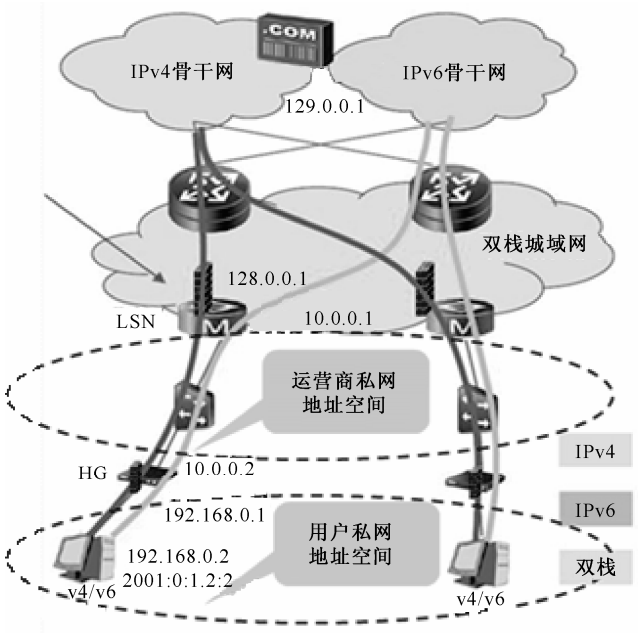



图 4-6　私网双栈+NAT444 方案

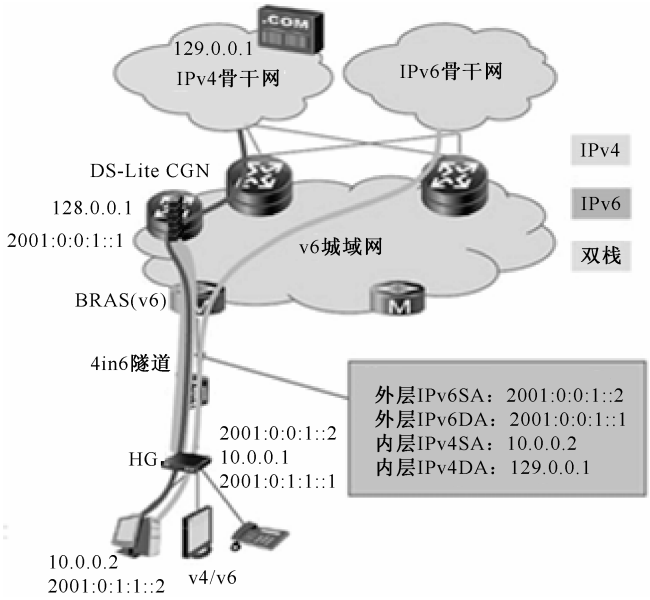



图 4-7　DS-Lite + NAT44 方案

该方案要求 CPE 终端支持双栈，分配一个 IPv4 私网地址、一个 IPv6 地址。

采用 DS-Lite 方案的一个好处是减轻宽带接入服务器设备的压力，可以只运行 IPv6 协议栈，适合在 IPv6 占主导地位的应用场景下使用。

（3）方案三：6rd

6rd 是 IPv4+6over4 隧道的典型方案，类似的解决方案还有 IPv6 over L2TP（通过 L2TP 隧道来提供 IPv6 用户远程接入）。6rd 是基于 IPv4 网络快速引入 IPv6 的方案，现有城域网络的宽带接入服务器等设备不用升级改造以支持 IPv6，在城域网络中集中部署 6RD 网关，6RD 网关到骨干网之间建立 IPv6 连接，用户的 CPE 需要支持 6RD。当用户有 IPv6 接入需求时，CPE 与 6RD 网关之间建立 IPv6 over IPv4 的隧道，IPv6 通过隧道转发到 6RD 网关，而用户的 IPv4 访问继续通过原有的路径实现。该方案适用于 IPv6 业务发展的早期，运营商以 IPv4 业务为主，拥有少量的 IPv6 用户。

6rd 方案如图 4-8 所示。

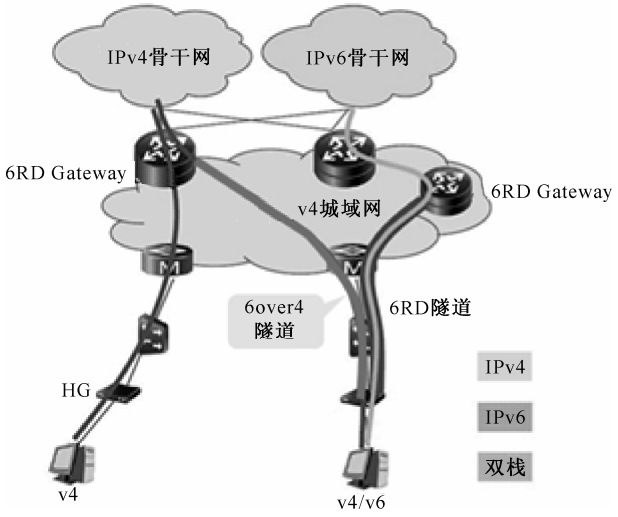



图 4-8　6rd 方案

**表 4-4　三种过渡方案的比较**

| | 私网双栈- NAT444 | DS-Lite+NAT44 | 6rd |
|---|---|---|---|
| 技术成熟度 | 已标准化 | 已标准化 | 已标准化 |
| 产业成熟度 | NAT44 在现网已规模部署，产品成熟 | 尚未规模部署，设备能力还有待验证 | 在部分欧洲运营商规模部署 |
| 对现网影响 | 较小 | 较大，需要在局端实现 DS-Lite 隧道、翻译（44）功能 | 较大，需要在局端实现 6rd 隧道、翻译（64）功能 |

续表

| | 私网双栈- NAT444 | DS-Lite+NAT44 | 6rd |
|---|---|---|---|
| 客户端 CPE 设备的要求 | 私网地址空间翻译 | 支持 DS-Lite 隧道 | 支持 6rd 隧道 |
| 客户端 IPv4 地址需求 | 私网 IPv4 地址 | 私网 IPv4 地址 | 公网 IPv4 地址 |
| 利于流量向 IPv6 迁移 | 否，流量承载在 IPv4 网络 | 是，流量（接入网）由 IPv6 网络承载 | 否，流量承载在 IPv4 网络 |
| 面临的主要问题 | 网络复杂，两级 NAT 增加了业务的复杂度；地址溯源难 | 局端设备会成为新的瓶颈（扩展性），需要大规模升级 CPE 家庭网关 | 需要大规模升级 CPE 家庭网关；应用需要支持 IPv6 |

（4）互通方案一：有状态翻译技术——NAT64+DNS64

NAT64+DNS64 是解决 IPv6 用户访问 IPv4 网络业务资源的一种有状态的翻译方案。在该方案中，用户端的应用、接入设备和网络均支持 IPv6，用户使用 IPv6 的业务和内容是直接的，但接入 IPv4 业务和内容将需要有状态的地址翻译（NAT64）网关设备。DNS64 则主要配合 NAT64 工作，将 DNS 查询信息中的 A 记录（IPv4 地址）合成到 AAAA 记录（IPv6 地址）中，返回合成的 AAAA 记录用户给 IPv6 侧用户。用户的业务流量将根据这个目的地址路由到 NAT64 网关设备，在此设备对目的地址和源地址进行地址和协议翻译，以 IPv4 分组包的形式路由到最终的服务器，具体如图 4-9 所示。

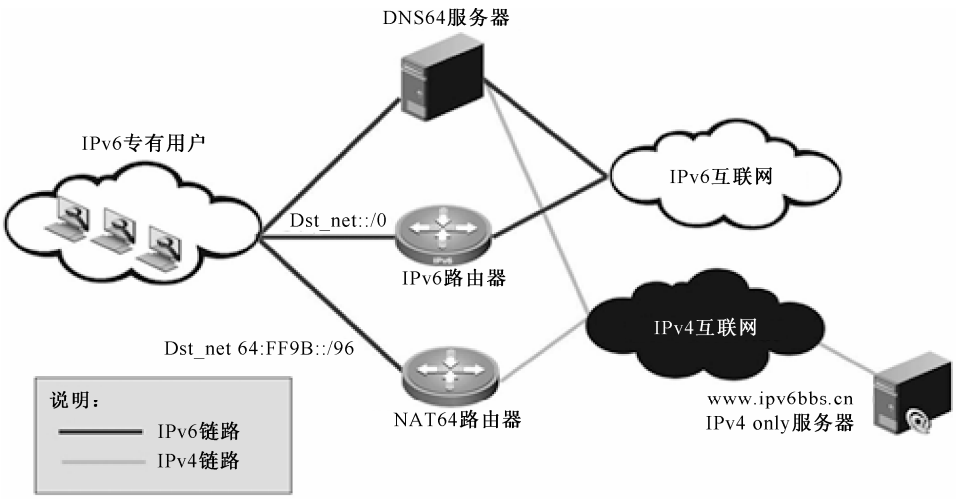



图 4-9　NAT64+DNS64 架构

（5）互通方案二：无状态翻译技术——IVI

IVI 是解决 IPv6 用户访问 IPv4 网络业务资源和 IPv4 用户访问 IPv6 业务资源的

一种无状态的翻译方案。该方案的实质是用已有一部分 IPv4 的地址段构造特定的 IPv6 地址段，通过将 IPv4 地址嵌入 IPv6 地址段的方法使它们形成明显和特定的映射关系。IVI 的功能主要有两个：一个是地址映射，即通过统一的规则实现 IPv4 地址与 IPv6 地址的一一映射，以进行地址的翻译；另一个是协议翻译，即根据标准规定，实现 IPv4/ICMPv4 协议和 IPv6/ICMPv6 协议各字段的对译，同时更新 TCP/UDP 协议的相关字段，完成完整的数据包翻译操作。

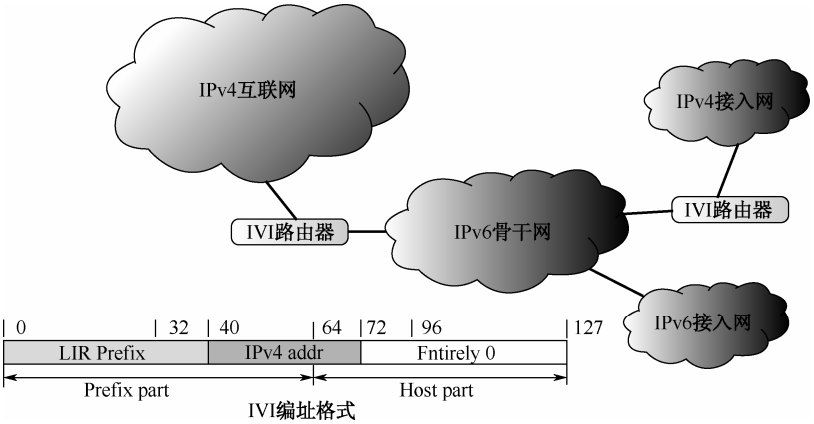



图 4-10　IVI 技术方案架构

**表 4-5　两种互通过渡方案的比较**

| | NAT64 | IVI |
|---|---|---|
| 技术成熟度 | 已标准化 | 已标准化 |
| 产业成熟度 | 尚未规模部署，产品成熟度有待验证 | 已在 CERNET2 上部署 |
| 地址格式要求 | 特定地址前缀，64:ff9b::/96 | 特定格式，IPv6 地址内嵌 IPv4 地址 |
| 业务访问 | 仅支持单向访问，即 IPv6 用户访问 IPv4 业务 | 支持双向访问，即 IPv6 用户访问 IPv4 业务、IPv4 用户访问 IPv6 业务 |
| 对域名系统的影响 | DNS 升级支持 DNS64 功能 | DNS 升级支持 IVI 功能 |
| 对现网的影响 | 较小，在有 IPv4/IPv6 互通需求的点部署 NAT64/DNS64 设备 | 较小，在有 IPv4/IPv6 互通需求的点部署 IVI 网关设备和支持 IVI 功能的 DNS 系统 |

# 第 5 章 未来网络核心问题及研究状况

**本章要点**

- ✓ 未来网络的网络架构
- ✓ 未来网络的业务支持能力
- ✓ 未来网络的外部能力
- ✓ 新型网络体系结构的研究现状与趋势
- ✓ 未来网络试验平台


IPv6 能够较好地解决现网 IP 地址资源不足的问题，但是制约现网发展的网络安全性、网络扩展性、网络移动性等突出问题并未得到根本性解决，为此，学术界和产业界的一些专家开始采用“Clean Slate”的思路，利用革命性技术路线，强化网络架构和基础协议的创新，试图解决下一代互联网中长期发展的技术方向问题，掀起了未来网络技术研究的新一轮热潮。

# 5.1 未来网络的网络架构

## 5.1.1 网络架构的核心问题：命名、编址、路由和资源管理

在数据通信的发展历史中，命名和编址一直都不是主要关注的问题。如果网络结构足够简单，而范围又十分有限，命名和编址就不是问题。大多数早期网络都是点对点或多站线路网络，因此寻址可以通过简单的枚举完成。即使是大型 SNA 网络，寻址也不是问题。因为 SNA 是分等级的，从叶（终端）到根（主机）只有一条路径，所以枚举层次结构（树）的叶子就可以了。实际上，在具有多路径的分散网络（如早期的 ARPANET 乃至早期的互联网）中，寻址都可以通过枚举实现。但是随着网络结构越来越复杂，命名和寻址成为必须面对的问题，和路由及资源管理问题一起成为互联网网络架构的核心问题。

关于互联网网络架构的这几个核心问题，在互联网发展的早期就有过很多理论研究。其中普遍得到大家认可的一个观点，是由 John F. Shoch 在 1978 年发表的一篇重要论文 *Inter-Network Naming*，*Addressing*，*and Routing*（该文章在出版之前就已经在 ARPANET 社区内部传阅了一年多）中提出的。文章认为，计算机通信中应当包含三个重要概念：（位置独立的应用程序的）名称，表示“我们在寻找什么”；（反映位置信息的）逻辑地址，表示“它在哪里”；路由选择，表示“怎样到那里”。此外，逻辑地址和下层的物理地址之间存在映射关系。互联网发展到现在，和这几个概念相对应的分别是：应用层的 URI（URL，URN）充当了应用层的命名角色，网络层的 IP 地址对应逻辑地址，路由选择也主要在网络层完成，MAC 地址则对应于物理地址，如图 5-1 所示。

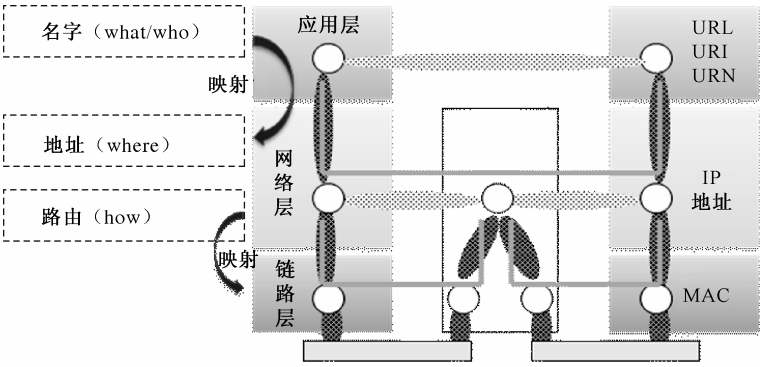



图 5-1　计算机通信的理想架构映射到现有的互联网架构

如果仔细分析这个对应关系，则会发现目前互联网中的编址、命名、路由和资源管理等核心架构都存在着问题。

### 1. 应用层缺乏命名机制

在图 5-1 所示的结构映射中，URL、URI 及 URN 等对应的是应用层的命名机制。然而 URI 等作为资源标识和位置紧密相关，将其看作应用层地址更合适，因此在应用层实际上缺乏位置独立的命名机制。

### 2. 网络层 IP 地址错误承担了双重语义

在现有的互联网架构中，IP 地址既作为位置标识又作为身份标识，具有双重语义。从传输层和应用层来看，IP 地址代表身份信息，用来标识一次端到端的连接；从网络层来看，IP 地址代表的位置信息，用来在网络中进行路由和寻址。在互联网发展初期，以 IP 地址作为终端的身份标识可以充分利用 IP 地址全球唯一的特性，避免引入新的名字空间，简化了传输层协议的设计与实现。然而 IP 地址的实质是对接口（Interface）的编址，会随着位置的变化而变动，因此作为名称，无法做到位置独立；IP 地址作为地址时，由于目前 IP 地址全局分配和申请方式，IP 地址更多地反映的是运营商信息，因此既不能像电话系统一样完全反映地理位置信息，又不能像操作系统逻辑地址一样做到严格分层。

### 3. 互联网路由面临严重的可扩展性问题

造成路由扩展性问题的深层根源是当前 Internet 架构中的 IP 地址承担了双重语义，既表示主机身份（用于传输层表示会话的端点），又表示主机位置（用于路由系统进行数据包的路由寻址）。根据 Rekhter’s Law，为了保证路由系统的可扩展性，IP 地址分配应该与网络拓扑相适应。但由于 IP 地址同时承担主机身份的角色，地址

分配往往是基于组织结构的（而不是拓扑结构的），而且相对稳定，不能根据网络拓扑的改变而动态调整。这两种角色的目标不统一，使得单一 IP 地址命名空间难以同时满足双重角色的要求，从而产生了路由扩展性问题。

#### 4. 互联网资源管理矛盾重重

目前互联网的基础网络资源有两类：一类是用于开展 Web 浏览、电子邮件、虚拟网络社区等互联网基础应用的域名资源；另一类是目前用于主机和位置标识的 IP 地址资源。然而目前域名系统的管理权受发达国家控制，互联网域名与号码分配机构 ICANN 位于美国，13 个根服务器也都位于发达国家；IP 地址的分配方式过于单一，由于目前 IP 地址全局分配和申请方式更多地反映的是运营商信息，既不能像电话系统一样完全反映地理位置信息，又不能像操作系统逻辑地址一样做到严格分层，客观上造成了 IP 地址语义的扭曲。

总而言之，目前构成互联网核心架构的命名、编址、路由和资源管理这四个方面存在着应用层命名机制不完善、网络层地址承担双重语义、路由扩展性问题严重及互联网资源管理矛盾重重等问题。互联网核心架构的问题已经成为目前互联网许多其他问题的重要原因。一方面缺乏命名机制使得互联网对于移动性支持能力先天不足，尽管目前出现了一些解决移动性的方案，如 MobilIP 和动态 DNS 等，但是实现起来难度较大，此外“多宿主机”的出现也使得问题更加复杂。这些问题已经成为制约互联网发展的瓶颈。

### 5.1.2 命名问题解决思路：建立统一命名与映射机制

在未来网络中，网络标识和用户身份标识是一定要区分的，这也是网络与业务分离趋势的必然要求。但是同时应考虑到业务标识与网络标识、身份标识的关系。未来网络支持的业务多种多样，为了简化操作、便于用户使用，最好用户只需记住一个便于记忆的身份标识即可，业务标识和网络标识由运营商来维护和管理，从而能够提供类似 ENUM 和“一号通”的功能。综合起来，未来网络编址命名系统的重要方向是对网络资源的统一命名与快速映射机制相结合，正本清源，回到最开始的设想，即在应用层为用户提供一个与位置无关的身份标识，网络层地址则承担位置标识的功能，命名和编址功能划分清楚、定位清晰，同时建立二者之间的快速映射机制。在这一大方向下，存在着以下三种技术思路。

#### 1. 基于现有互联网映射机制的应用层命名系统

在应用层为每个实体分配唯一可标志的资源标志符，资源标志的语法定义了用于命名网络资源的字符集及构成规则；字符集合语法规则决定了互联网资源名称名字空间的范围和大小，所有互联网资源名称的集合构成名字空间。利用现有的 DNS

系统在资源名称和 URI 之间建立映射，建立基于 URI 的寻址体系。这方面代表性的方案有 W3C 提出的 XRI、UDDI 等技术。

基于现有互联网映射机制的应用层命名系统如图 5-2 所示。

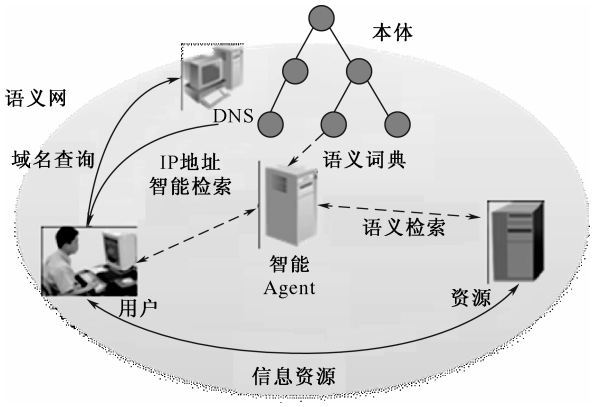



图 5-2　基于现有互联网映射机制的应用层命名系统

### 2. 基于分布式映射的命名系统

基于内容产生的内容标识符用于应用层命名，应用或节点的名字不会随着位置的改变而改变，从而在应用层解决移动性问题，并通过基于分布式的查询系统直接实现应用层命名和网络层节点地址之间的高效映射，具备良好的扩展性。这方面代表性的方案有 Berkeley 提出来的 I3 网络。

基于分布式映射的命名系统如图 5-3 所示。

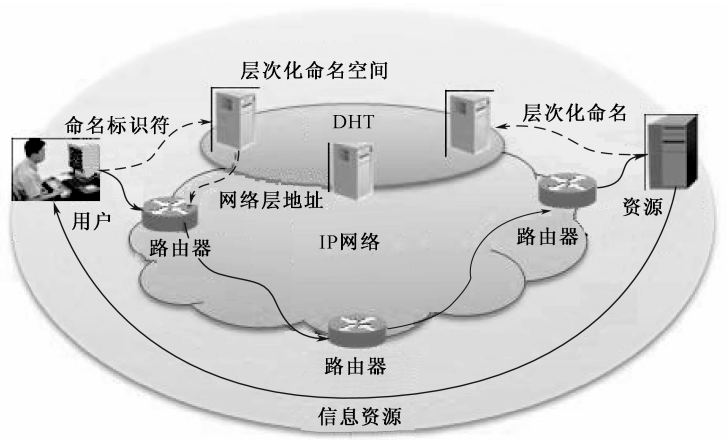



图 5-3　基于分布式映射的命名系统

### 3. 基于名字的内容路由

应用层和网络层相融合，建立层次化命名空间，将内容映射为内容标识符，作为命名，直接基于名字的内容路由。这方面有代表性的方案有 NDN（Named Data Networking）网络等。

基于名字的内容路由和传输控制如图 5-4 所示。

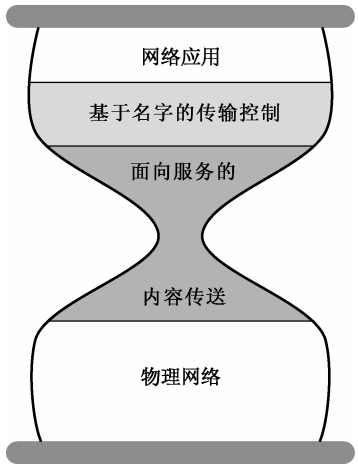



图 5-4　基于名字的内容路由和传输控制

## 5.1.3　编址问题解决思路：建立具有高可扩展性、语义清晰的编址体系

目前的 IP 地址存在着语法和语义两方面的问题。IP 地址的语法指的是地址的语法结构，包括包头设计、地址长度等；IP 地址的语义则指 IP 地址所承担的角色、地址分配的机制等。

从语法角度看，目前 IPv4 地址长度只有 32 位，其地址容量已经不能适应互联网的发展。目前 IANA 地址池中的 IPv4 地址已经分配殆尽，RIR 中的存量地址预计将在 2 年内耗尽，地址扩展性问题成为当前互联网发展最需要解决的问题之一。

从语义角度看，互联网地址需要解决 IP 地址承担双重语义的问题。IP 地址既代表身份信息，用来标识一次端到端的连接；又代表位置信息，用来在网络中进行路由和寻址。这种二义性导致了路由扩展性、移动性和多宿等多个问题的产生，成为制约互联网发展的瓶颈。

对于这些问题的解决思路，主要有以下三个方向。

**1．不改变 IP 地址的语法和语义，通过一些修补措施改善目前的地址短缺问题**

这种演进型思路主要有三类技术：一是提高现有地址利用效率，这类技术以无类域间路由（CIDR）、动态分配 IP 地址和可变长子网掩码（VLSM）为代表；二是地址翻译技术，以私有地址/网络地址翻译（NAT）为代表；三是地址嵌套技术，以 IP in IP tunneling 和 DS Lite 等技术为代表。这些修补措施可以在短期内缓解地址短期问题，但是不能从根本上解决问题。大量地址复用技术的使用将更快地恶化全球互联网的运行和发展环境，使网络的复杂性加速增加，导致业务创新、部署和运营成本不断攀升，同时也给溯源等安全问题带来新的挑战。因此要彻底解决地址的可扩展性问题，必须改变 IP 地址的语法结构。

**2．重塑网络层地址的语义和语法，统筹解决地址可扩展性、地址语义模糊及衍生的路由可扩展性等问题**

这种革命性思路的一类典型技术就是地址结构层次化思想。重新设计地址结构，实现网络层地址的层次化（按照网络拓扑层次或按照地理区域层次）语义，并包含节点势能等路由信息。设计地址结构时，扩大地址长度，可以解决地址可扩展性问题；地址结构中包含了地理区域等信息，明确了网络层地址应该承担的位置功能，解决了地址语义不清晰等问题；利用地址字段的交换替代路由，可以解决路由扩展性等问题。这种既改变语法又改变语义的革命性思路，需要对当前的地址体系做彻底的改变和创新，这个过程会涉及网络改造的方方面面，目前还处于研究和试验初期，距离大规模的使用和公众普遍接受还有相当长的路。

**3．保持 IP 地址的语义，通过改变语法彻底解决地址短缺问题，在易用性、组播、服务质量等方面有创新空间**

这个融合性思路的典型代表就是 IPv6 技术。和演进性思路的解决方案相比，IPv6 具有几乎无限的地址空间，可以保证 IP 网络端到端的透明性，简化网络结构，可以彻底解决地址可扩展性问题；和革命性思路相比，IPv6 是全球唯一发展较成熟的、可供产业界规模部署应用的技术。因此，IPv6 的部署是现阶段互联网演进的最好选择，也是必然选择。然而 IPv6 目前主要解决了互联网发展中的地址短缺问题，而在路由扩展、安全可信、服务质量保证等其他方面相比 IPv4 却没有实质性的改善，因此 IPv6 部署之后，还会经历一个技术演进阶段，需要在多个技术领域取得突破。

## 5.1.4　路由问题解决思路：改扁平路由机制为层次化路由体系

现有路由体系结构最突出的问题是扩展性问题。APNIC（Asia-Pacific Network Information Center，亚太地区网络信息中心）提供的 BGP（Border Gateway Protocol，

边界网关协议）路由表数据分析报告显示，当前 Internet 路由数量增长迅速，截至 2010 年 12 月，IPv4 的 BGP 路由数量达到了 336 364 条，如图 5-5 所示。业内专家甚至大胆预测，到 2020 年 Internet 路由表将达到 200 万个。

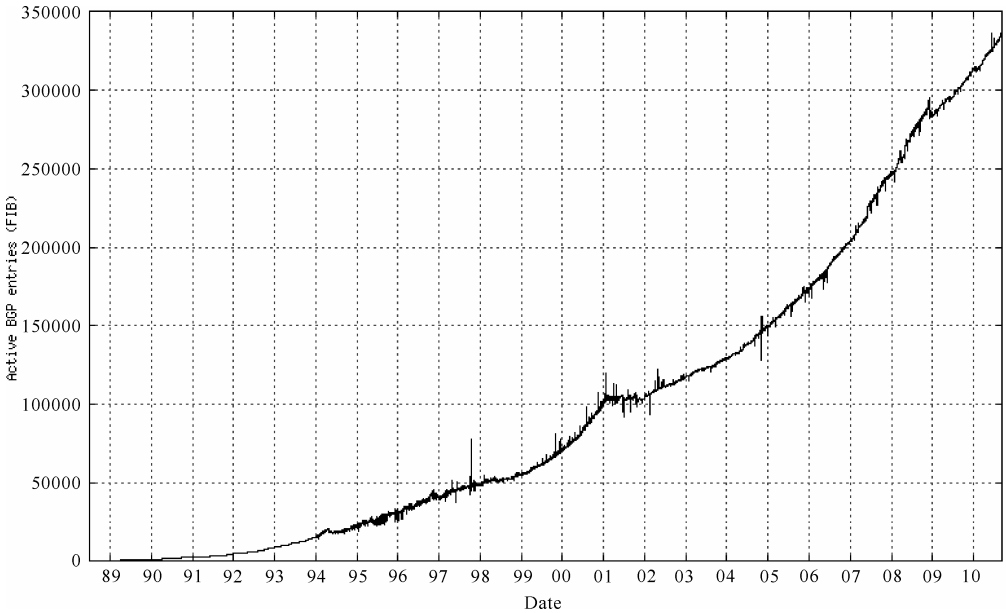



图 5-5　全球路由表规模快速膨胀

造成路由可扩展性问题的原因有多种，如图 5-6 所示。包括：网络/用户规模的高速发展，运营商独立地址广泛使用，IPv4/IPv6 长期共存，IPv4 地址交易不断加剧，网络多归属和流量工程的广泛使用及 IP 地址承担双重语义等。其中最根本的原因还是 IP 地址承担双重语义。


图 5-6　路由可扩展性问题的原因和后果

路由表的快速增长会为互联网的发展带来严重后果：域间路由收敛变慢，网络稳定性下降；制造商研发成本和运营商投资成本增加；设备能耗增加，不符合节能减排趋势等。

为解决现有互联网存在的路由扩展性等问题，整个业界开展了关于路由体系架构的研究活动，并提出了大量研究思路与方案，根据技术原理依然可以将重要方案归纳为演进性思路和革命性思路两个方向。

演进性思路不改变 IP 地址的语义，通过一些修补性措施来缓解路由可扩展性问题，具体技术如下所述。

### 1．边缘用户网络与运营商网络分离（Map/Encaps）

该思路将 ISP 网络（RLOC 标识，Routing Locator）和边缘用户网络（EID 标识，Endpoint ID）分开，核心路由器上只保留 ISP 网络的全局可路由地址，数量庞大的边缘用户地址将从核心路由器中剥离出来，从而大大减少路由数。本地网络路由基于本地位置标示（唯一身份标示和本地寻址）进行，当数据包进入核心网络时，必须通过编码器加上 RLOC。核心网络的路由基于 RLOC 进行，一旦数据包进入 RLOC 标识的 ISP 网络，本地路由将重新接管并完成最后的传递。初步规划只为具有重要互联链路的 ISP 分配 RLOC，而全球只有不到 10000 家这样的 ISP，并且这一数字的增长率远低于路由表的增长率。其代表方案有思科的 LISP（Locator Identifier Split Protocol，位置与标识分离协议）方案及华为提出的支持增量部署的 VA（Virtual Aggregation，虚拟聚合）方案等。

这类方案虽然有助于缓解路由扩展性问题，但带来了一些新问题，如需要对所有 IP 包增加一次隧道封装，要执行 Identifier 与 Locater 之间的映射，庞大的映射数据库的生成、分发、查询，首个数据包可能出现的超时，新协议的部署，等等。这些问题都是全局性的，会给网络带来很大的负担和开销。

### 2．身份标识与位置分离（ID/Locator）

该思路主张彻底分离身份标识和位置信息，地址仅用于标识位置，提供全局路由，而身份则采用新的名字空间。主机发送数据包时添加源和目的位置标识，在后续的网络传送中仅以位置标识进行路由。当身份标识到位置标识的映射发生变化时，由主机向分布式映射数据库通告。主机从映射数据库请求并缓存所需的标识映射关系。如果在现有 IP 网络中定义全新的用户标识，IP 地址就可以完全按照网络拓扑部署，便于 CIDR 地址聚合，从而彻底解决路由扩展性问题。其代表方案有 Ericsson 的 HIP（Host Identity Protocol，主机标识协议）方案及华为提出的 HRA（Hierarchical Routing Architecture，分级路由架构）方案等。

身份标识与位置分离的方案实现了 IP 地址双重语义的彻底解耦，能够解决移动

性、网络多归属等问题，增强了安全性，实现了路由系统的可扩展，但是这类方案需要对主机进行修改，部署难度较大，不能支持有效的流量工程和组播，此外协议开销较大，尤其是在带宽资源受限的移动应用场景中。

### 3．地理位置聚合

基于物理地域来聚合位置标识，可以按不同方向将路由信息进行汇聚。由于不需要洪泛具有位置标识功能的可达性信息，这种方案可以大大减少路由表的条目数。问题在于其不符合互联网商业模式、需要建立区域互联点。

### 4．转发表压缩

Internet 路由方式完全不变，继续沿用 BGP 协议。但在生成 FIB 表时，使用算法对转发条目进行压缩。该方案虽然不能改善控制平面的扩展性问题，但可以大大提高转发平面的扩展性。问题在于 RIB 扩展性没有解决、核心网 FIB 未必能聚合。

革命性思路改变 IP 地址的语义和语法，重新设计地址结构，建立新的路由体系架构。

路由体系架构的问题根源在于 IP 地址所承担的双重语义，IP 地址既表示主机身份（用于传输层表示会话的端点），又表示主机位置（用于路由系统进行数据包的路由寻址）。根据 Rekhter’s Law，为了保证路由系统的可扩展性，IP 地址分配应该与网络拓扑相适应。但由于 IP 地址同时承担主机身份的角色，地址分配往往是基于组织结构的（而不是拓扑结构的），而且相对稳定，不能根据网络拓扑的改变而动态调整。这两种角色的目标不统一，使得单一 IP 地址命名空间难以同时满足双重角色的要求，从而产生了上述路由扩展性问题。语义混淆还会进一步使移动性、多归属、流量工程及安全性问题复杂化。因此革命性思路的出发点就是重新设计地址结构。

革命性思路的代表技术之一是层次化交换。目前互联网用的是 Mesh（任意连接）结构，没有中心和层次，无序的网络体系结构使得 IP 包的寻址不得不依靠路由技术。如果重新设计地址结构，将互联网改造成层次化结构的，并把地址与网络结构相关联，利用地址字段的交换替代路由，路由扩展性等问题自然也就得到了彻底解决。

革命性思路的代表技术之二是明确地址的位置信息。通过改造地址结构，在地址中包含节点的地理位置信息及势能信息。在节点寻路时，则可以不依赖日益膨胀的路由表信息，而是根据节点的位置信息和势能信息确定路由，从而解决路由扩展性问题。

虽然革命性思路和演进性思路的出发点不同，但不能就此说二者是矛盾的。一方面，革命性思路虽然尚未成熟，但其对于演进性思路将会有积极的影响；另一方面，演进性思路对于如何建立全新的体系架构、提高创新效率、防止走弯路也具有

重要的借鉴意义。二者是对立统一的关系。就路由扩展性问题来说，革命性思路和演进性思路都将核心与边缘分离、身份与位置分离作为核心思想，并有可能向这个方向融合。

### 5.1.5　资源管理问题解决思路：建立民主的互联网资源管理机制

当前的互联网资源管理问题重重，单一的地址分配模式一方面造成了地址分配无序，另一方面无法反映位置信息，造成了 IP 地址语义模糊；域名管理受发达国家控制，管理中枢 ICANN 位于美国，根服务器全部位于发达国家，为发展中国家的互联网安全带来隐忧。

互联网不仅是生产力，也是与货币、能量并列的第三通货。互联网应该反映市场主流意识，体现世界核心利益，焕发人类创新精神，避免一国独大，建立民主的管理机制。互联网资源管理问题大体可以有以下四种发展模式。

#### 1. 继续维持以 ICANN 为主的互联网社团治理的模式

这个模式的核心实际上是维持了以美国为主的根服务器的解析模式，它的局限性是向主权性、私密性市场扩张受到限制。倘若国际社会以互联网市场发展为第一目标，这个模式就需要与时俱进、包容各种挑战和转变。

#### 2. 实行以多个国际组织共同治理的模式

即从一国一组的 ICANN 管理模式转变为多国多组的国际化模式，这个模式的核心是通过不同国际组织实现根服务器管理的扩大化、自主化，可以兼容能源网、金融网、环境网等安全性的需求，这个模式的转型红利是以互联网管理有限度的民主化换取了市场的扩张化。

#### 3. 参考国际电信联盟 ITU 的编号、命名、寻址和识别资源的分配和管理程序，建立以主权国家为主的互联网域名管理互联互通的机制

例如，可参考 ITU 之 E.164 标准所分配的国际长途电话区号模式。这个模式的核心是可以建立以各国家或有关地区为主的松散的根服务器管理模式，它的转型难点是如何启动并管理这个体系。

#### 4. 将现有的互联网改组重组为大国治理模式

例如，以作为世界主要互联网中心的大国或大国联盟为基础的协调机制；或者重组为以 G20 国家为基础的合作机制；或者以其他混合机制为基础而造就的主要国家责任制模式。这个模式的核心是将现有的以美国为幕主、以 ICANN 为运营主体的

互联网社团治理模式演化为大国责任制。它的优点是既解决了互联网的民主化，又解决了互联网的市场化，特别是落实了互联网升级的资本积累和新技术扩张的市场。

以上四个模式反映了与主权国家或国家联盟对应的主权利益，契合了互联网是与海洋、太空并列的全球共享的财产的基本特征。这四个模式更多地属于一种发展框架模型，最终可能形成几个模式的复合发展；或可将多个模式重组为分步实施的交叉战略，应该具有“答复互联网应该是什么的哲学思考，又应该包含着互联网将会是什么的科学判断，也必须提供互联网可以是什么的创新资源”的主要特征。

## 5.2 未来网络的业务支持能力

IP 协议在设计之初只考虑了主机之间的点到点通信的问题，对更通用的通信模式（如点到多点或广播）、更复杂的网络结构（如用户的多接入）、更多样化的业务需求（如终端移动性等）考虑不足。因此当这些多样化的需求出现之后，当前的互联网中也出现了多种改良性的解决方案，但这些改良性方案都只是在现有互联网体系上的修补，无法从根本上解决问题，同时还会引入一定的复杂度；同时从革命性路线的角度来看，虽然有众多创新的想法，但短时间内还无法落地。本节结合两种路线的解决思路，提出了一些解决网络业务支持能力问题的可行方案。

### 5.2.1 多宿问题的解决：新的编址及路由机制

所谓多宿，即用户出于安全或服务质量方面的考虑，将自身网络使用自带地址同时接入两个以上的运营商网络。这种情况下，在互联网骨干层面将出现多份路由，增加了骨干层的路由扩展性压力。据统计，目前全球共有 30 000 多家企业和机构采用了多宿的接入方式，不仅给互联网带来了沉重的路由负担，同时这些客户网络的变化也造成了骨干层面路由的频繁振荡，目前全球路由表的更新频率已经达到每秒 6 次，每天 50 万次的水平。

对于多宿问题，基于目前的 IP 路由技术提出了一些路由层面的解决方案，如“自动路由注入法”、“隧道封装法”等，这些方法虽然能够在一定程度上减轻用户都接入对互联网核心层面的路由压力，但需要在现有路由协议上增加判断和处理机制，增加了设备处理的负担。

多宿问题的本质是互联网核心层面的路由扩展性问题。在创新性互联网架构（如层次交换网络体系、未来包交换网络（FPBN）、I3 等）之中，提出了通过改变地址语义和结构（如层次化地址）、改变路由方式，从根本上解决互联网核心层的路由扩展性问题，从而减小多宿问题的影响。从这一点上来看，多宿问题的解决最终还是要依靠新的编址和路由机制。

解决多宿问题的改良型方案如图 5-7 所示。

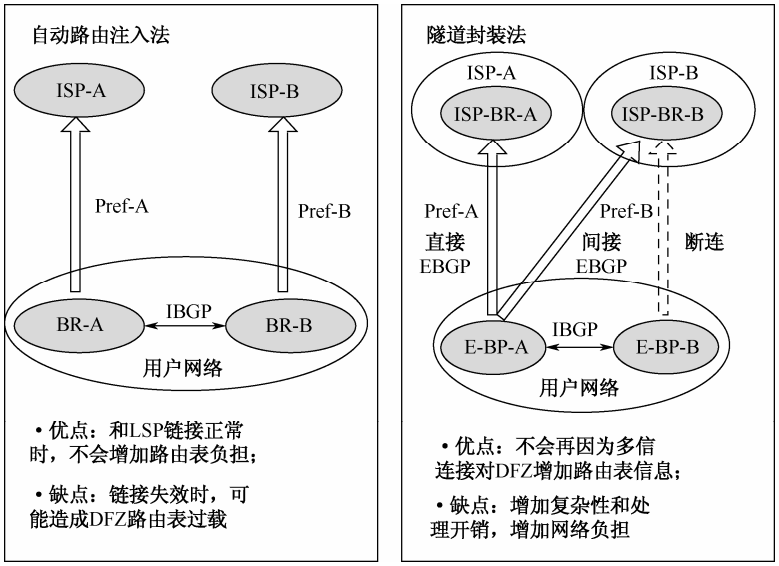



图 5-7　解决多宿问题的改良型方案

## 5.2.2　组播问题的解决：应用层组播

目前的互联网在设计之初只考虑了点到点通信，即单播的问题，并没有考虑网络中出现点到多点甚至广播型业务的场景。在 IPTV、视频会议等点到多点或多点到多点业务需求出现之后，人们在单播路由协议的基础上设计了组播路由协议，利用单播路由生成的最短路径树生成组播路由，以单播的方式解决组播的问题。这种方式的缺点在于组播汇聚点和流量复制点压力大，而且组播协议本身灵活性有限——PIM-DM 基于洪泛再剪枝的方式，效率较低；而 PIM-SM 采用显式加入的方式，加入、离开的延迟较大。目前为了保证组播业务的质量，更多地采用静态组播的方式，直接将组播流量推送到所有网络边缘节点，但这种方式又造成了网络带宽的浪费。

在众多革命性路线的思路之中，人们已经提出了很多全新的网络体系架构，如 NDN、I3 等。这些网络体系采用了发送与接收过程分离的思想，将点到多点作为基本的数据传送模式，发送节点只是将数据发送到网络中，接收节点根据其需要对数据及资源进行申请，再由网络节点将数据发送至接收节点。

革命性路线通过对路由机制的革新，解决了点到多点的问题，但与此同时，点到点的通信反而成为较难解决的问题，在这一点上，基于“发送与接收过程分离”的思路目前还没有很好的解决方案。但与此同时，已经出现了一些从应用层来解决点到多点通信问题的方案，如 CDN、P2P 等，这些应用层技术的出现给我们提供了

另外一条思路，同时理应成为未来一段时间的研究重点。

NDN 和 I3 的数据发送模式如图 5-8 所示。

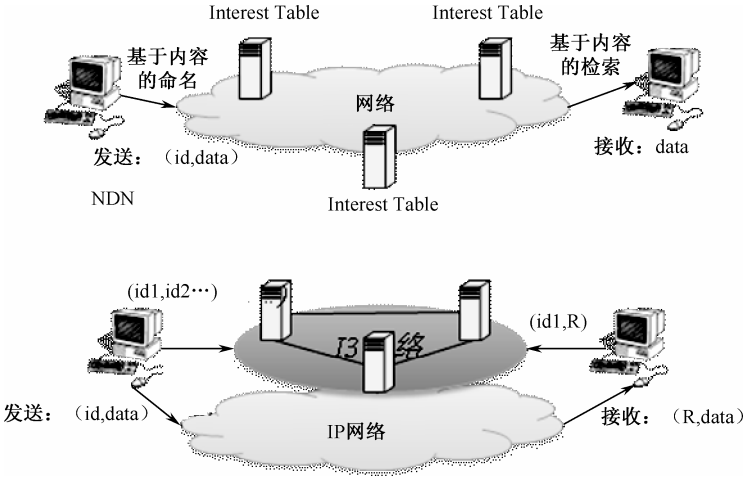



图 5-8　NDN 和 I3 的数据发送模式

## 5.2.3　移动性支持问题的解决：应用层实现

无线数据接入技术的出现使终端摆脱了线缆的束缚，可以自由地接入互联网络，但同时催生了终端移动的需求，用户希望在终端的移动过程中应用（尤其是一些关键性应用，如金融交易等）不会中断。但目前的 IP 地址对于应用来说既充当了节点的地址，又充当了应用的名字，因此无法满足节点移动最基本的名字与地址分离的要求；而现有的名字-地址映射机制——DNS 机制又显得过于缓慢——DNS 的更新时间为 8～12 小时，根本无法满足节点快速移动所带来的名字与地址的高速映射需求。

为了解决移动性问题，在几年之前就已经出现了“移动 IP 协议”（Mobile IP），这种解决方案通过三角路由的方式，使数据包首先经过主机的“家乡站点”，再通过隧道转发至漫游地。这种解决方案不仅效率低，而且协议流程复杂，因此并未得到广泛应用。

在众多革命性路线的思路之中，应用或资源的名字与节点地址的分离是最基本的想法，同时通过高效的映射技术（如利用 DHT 技术）使名字与地址之间的映射实现高速更新，从而满足节点移动的需求。

应该说实现名字与地址分离是解决移动性问题的根本方案，但从现实需求来说，对节点移动性提出严格要求的应用并不多，大多数对质量或接续过程并不敏感的应用实际上可以通过客户端保持状态并发起重传的方式在节点移动至新网络时使用户

保持较为连续的业务体验。

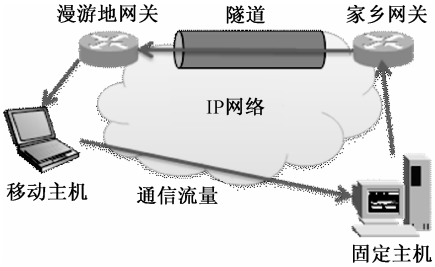



图 5-9　Mobile IP 协议流程

# 5.3　未来网络的外部能力

## 5.3.1　安全可信

早期的互联网被默认为“安全的网络”，因为传统互联网默认其用户群体主要是彼此相互信任、目标一致的团体，安全问题未得到设计者的重视。但是随着互联网的商用化和全球爆炸式发展，其用户群体在规模、目标、素质等方面各不相同，用户间的信任不复存在。互联网上病毒、网络攻击频繁发生，隐私无法保证，互联网被默认为“不安全的网络”。

当前，尽管学术界和工业界提出了一些解决方案（如解决域名系统安全问题的 DNSec、解决端到端通信保密问题的 IPSec、提供真实源地址的 SAVA、实现业务分析与识别的 DFI/DPI 技术等），但由于原有互联网体系结构缺乏整体安全框架，各种安全技术以“补丁”的方式添加，难免出现安全漏洞或功能重叠，甚至顾此失彼。

各种革命性路线的方案纷纷将保证网络的安全可信作为最基本的需求，同时提出需要一整套“安全架构”来保障网络的安全性，但从目前的研究成果来看，这些“安全架构”的体系仍未清晰，短期内很难落地。

因此，应对现有网络的问题需要借鉴革命路线的思想，从增强网络控制能力的角度设计可实现的解决方案，以下提出一些基本的思路。

### 1．构建网络安全顶层架构

分清终端、网络、应用的职能，对于不同职能的功能实体提供不同的安全保障级别和方案。

#### 2．通过资源隔离来保障安全

不追求全程全网的安全保障，而是通过资源隔离的方式将有不同安全需求的业务进行隔离，在不同的平面上各自提供安全保障。这样一方面能最大限度地满足业务的需求，同时能够避免不同业务之间的影响。

#### 3．研究针对特定业务的安全技术

重点针对一些关键性业务的特殊需求，如物联网、云计算等，优先研究有针对性的安全技术。

#### 4．减弱 IP 端到端的透明性

IP 的端到端透明性是导致互联网安全问题的重要原因，通过一些技术手段减弱网络的透明性，使网络能够对用户的业务应用进行一定程度的感知和控制，有利于提高网络的安全性。当然，网络的中立性与公正性也是需要考虑的问题。

### 5.3.2 服务质量保障

传统互联网体系结构中，核心网络只保存有限的管理信息，不提供 QoS 保证。随着互联网的商业化，大量实时应用涌现出来。视频会议和 IPTV 等多媒体应用对延迟、延迟抖动、带宽等有严格的需求，需要网络提供相应的服务质量保证。现有的 QoS 保障模型，如 IntServ/DiffServ、多协议标签交换（MPLS）、QoS 路由等，由于也属于以“补丁”的形式加入网络体系结构中的，在实际应用与部署中存在一些问题。例如，IntServ 扩展性差和管理开销大，DiffServ 则无法为每个数据流提供 QoS 保障。

#### 1．轻载模式不能支持互联网长期可持续发展

服务质量问题是困扰互联网发展的长期问题。虽然经过 20 多年的研究，也提出了许多服务质量方面的技术、标准和解决方案，但是从整体上来看，互联网还是利用轻载（best effort）来保证服务质量的。目前互联网基本上也能很好地支撑视频业务的开展，这得益于近几年网络基础设施能力和水平的快速提高，网络处理芯片和网络设备能力大幅提升，网络管理水平不断提高。但是应该看到，目前互联网的业务发展整体上看还处于初级阶段，随着以后互联网普及率的不断提高及其与生产生活方式的紧密结合，互联网的业务将日新月异，互联网流量将急速增加。

在不久的将来，互联网流量增加速度将会显著超过互联网网络基础设施能力的提高速度，互联网流量将变为稀缺资源。目前利用轻载方式实现的互联网流量的粗放管理方式将不可持续发展。

首先，轻载模式不节能环保——轻载方式简化了协议和实现，但带来了资源利用的不均和浪费；其次，轻载方式不总有效——统计复用将不可避免地带来局部瓶颈，局部的拥塞将使轻载失效；最后，轻载方式不能满足综合业务需求——轻载无法实现差异化服务。

### 2．互联网服务质量问题是互联网的基因性问题

20 多年努力失败的根本原因就是互联网的服务质量不是一个外部问题，而是和互联网的核心技术——编址路由密切相关的。要想从根本上解决互联网服务质量问题，就必须修改互联网基因——编址与路由机制。

（1）包交换网络的统计复用特性——链路利用率严重不平衡，很难针对链路进行带宽设计和“精确”的带宽控制。

（2）通信路径的不确定性——无序的网络拓扑结构和动态非确定性路由。对于无连接模式，路径的不确定性使得无法按照路径进行资源预留，如 DiffServ 技术只能实现节点级的资源管理，缺乏必要的接纳控制；QoS Routing、Backup-Path Routing 虽然解决了路径 QOS，但是成本高。对于面向连接模式，连接建立过程中的资源预留和管理的代价太高，如 RSVP 及 MPLS-TE 均因为复杂性而未获得成功。

（3）业务流量的不可知性——互联网网络行为学的“幂律”和“自相似”两大结论没有实际指导意义。流量突发性是包交换网络的固有特征，网络与业务不可感知，业务与承载的完全分离成就了互联网业务创新，也制约了 QoS 实现。

### 3．互联网服务质量问题的关键是要处理灵活性与管理性之间的平衡

未来互联网服务质量问题的解决需要处理好“统计复用的灵活性”与“精细管理的严格性”之间的平衡。一方面要保留 Best Effort 及网络与业务分离所带来的业务灵活性，另一方面要考虑资源精细化管理所带来的高效率。

QoS 问题需要处理灵活性与管理性之间的平衡，如图 5-10 所示。

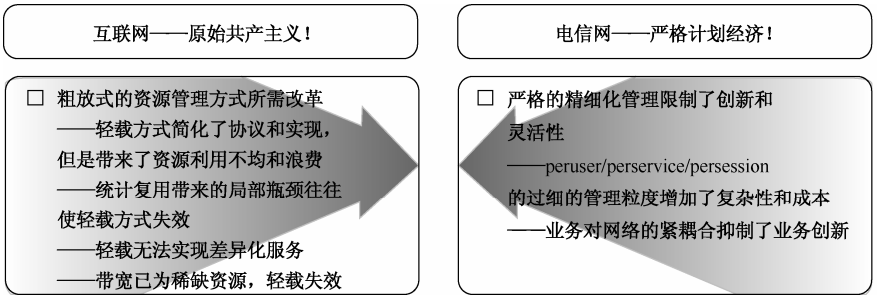



图 5-10　QoS 问题需要处理灵活性与管理性之间的平衡

### 4．未来互联网服务质量问题的解决要靠体系结构的创新

由于互联网服务质量问题是互联网的基因性问题，因此需要互联网体系结构上的

创新，通过研究新型的编址与路由机制来保证互联网的资源是可知、可管、可控的。

结构化地址和层次化网络结构是解决未来互联网服务质量问题的可行途径。地址的结构化地址和网络的层次化，可以取消全局路由，实现确定路由；可以通过网络逻辑分层，实现每层资源的相对独立，实现基于层的接纳控制、流量调度，有效控制复杂度。

## 5.3.3 绿色节能

随着互联网规模的不断扩大，包括网络设备、终端设备、IT 系统等在内的网络元素消耗着越来越多的能源。据统计，2007 年互联网能源消耗为 868 G 千瓦，占到了全球电力消耗的 5.4%，美国互联网的能耗已经占全国能耗的 9.3%，而且每年都以 8%～10%的速度增长。

面对愈加紧迫的节能压力，未来互联网必须从多方面考虑节能降耗的问题。未来互联网节能需要考虑终端/设备、网络技术、业务平台、网络布局等多个层面。

在终端和网络设备的层面，可以利用节能芯片，并通过系统软件的节能设计达到降耗的目的；从网络层来说，减少流量的迂回绕转，以及通过冗余路径休眠等方式可以有效降低数据流转过程中的能耗；从业务层面来说，利用云计算、虚拟化等技术可以提高资源的利用效率，减缓能耗的增长；在网络布局方面，需要统筹考虑网络与能源资源的布局，在资源富集地重点建设数据中心等耗能水平较高的网络基础设施，将传送“瓦特”变为传送“比特”，提高资源利用效率。

互联网节能降耗需从多个层面入手，具体如图 5-11 所示。

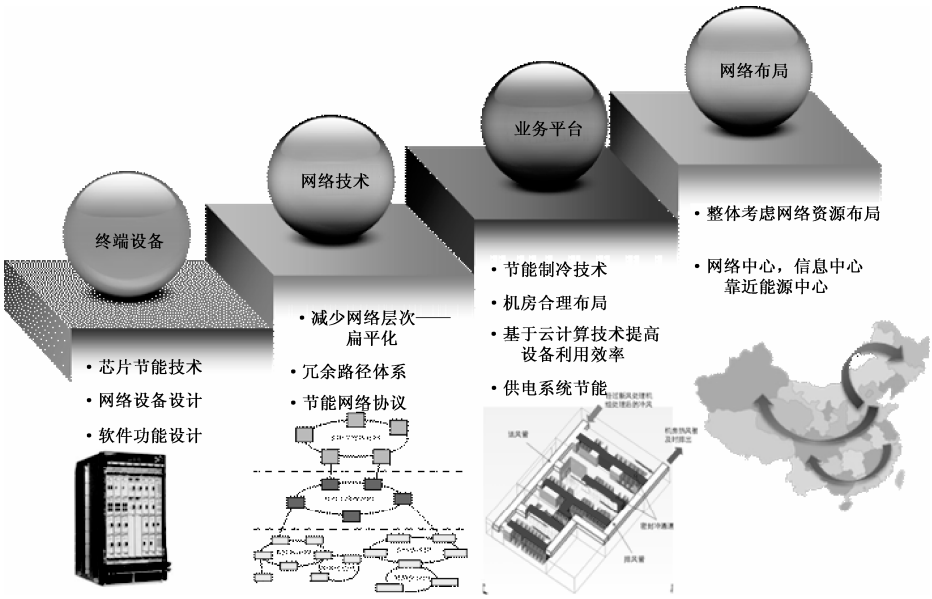



图 5-11　互联网节能降耗需从多个层面入手

# 5.4　新型网络体系结构的研究现状与趋势

综合前面几节的分析，当前互联网所面临的问题大多数难以以修补或完善的方式进行解决，因此我国还应加强创新性网络体系架构的研究，兼收并蓄，按照“未来网络技术要素模型”、以编址命名路由为核心寻求技术突破。

从国际国内未来互联网体系架构的研究情况来看，目前仍处在“百花齐放”的状态，从技术路线的角度看并没有一个统一的方向。因此我国也应保持技术方向的多样性，重点支持 3～5 种新型网络体系结构及其协议研究，选择国内有一定基础的技术方案，研发原型，进行试验验证，促进不同体系结构的共存、竞争与发展。

在未来互联网体系架构的研究中应体现协议的开放性和体系的开放性，重视网络操作接口的标准化，便于灵活地设计、开发和部署新网络协议。同时从可管理、可运营的角度出发，将认证、审计、溯源、过滤、智能防范等安全需求纳入下一代互联网安全顶层设计。

最后，应重视我国自主知识产权核心技术的国际化推广，积极参与下一代互联网的国际标准制定，推动具有自主知识产权的国内标准成为国际标准。

## 5.4.1　现有网络体系结构存在的问题

随着人们对信息服务需求的日益增长，未来信息社会呼唤可信赖、安全、可靠的网络与通信服务，而现有网络面对这些需求暴露出了诸多问题和深层次的矛盾，已经不能满足未来信息社会持续发展的需要。

### 1. 互联网的问题

互联网不能保证基本的安全性和可信任性，不可控、不可管、不能保证服务质量。

（1）互联网的不可信任性表现在设计、建设和运行管理的各个环节，频繁爆发的互联网安全事件是互联网脆弱性的具体表现。互联网的安全问题极大地限制了互联网更深层次的应用与业务的创新空间，并严重制约着互联网的发展及其巨大潜力的发挥，同时，也影响着国民经济的健康发展，甚至威胁着社会安定和国家安全。

（2）互联网本质上提供的是一种“尽力而为”的无连接的服务，不提供任何服务质量保证。在以 FTP、E-mail、Web 服务为主的数据业务环境下，互联网基本能够满足用户需求，但是面对语音电话、IPTV 等实时流媒体传递，以及大量终端出现移动通信的需求，已有的互联网难以提供足够的性能、功能和必要的服务质量。

互联网的核心理念之一是对于数据进行无记忆传送，在网络中尽量不保存或少保存状态信息，从而保证网络设备的简单和高效。这种理念使得网元中缺少用于管理的必要信息，使得管理员无法高效地对网络进行管理和控制。

### 2. 电信网的问题

传统电信网在多业务综合承载、新业务灵活部署等方面存在不足，基于 IP 内核的下一代网络（NGN）发展受到互联网基因缺陷的困扰。

现有电信网正在以 IP 为核心实施承载网的技术变迁，业务网将依托在以 IP 为技术基础的承载网之上已没有太多的悬念。然而，现有 IP 承载网不可控、不可管，不能提供服务质量保证，不能保证基本的安全性和可信任性，且加密技术滥用和失控，给信息通信安全造成了严重威胁；现有 IP 承载网的设计思路不能适应由于网络流量模型的变化而产生的新的业务承载需求。

当前电信业务建立在不可靠的 IP 网之上，业务网中存在大量不合理的功能；缺乏具有本国特色的创新型业务；电信领域和互联网领域的业务实现思路不同，优缺点各异，缺乏必要的融合与协调，未来业务实现思路尚不清晰，业务网成熟度和稳定性也不高；业务具体实现方式多样、混乱、易变，互联互通难度大；单独建设的多个业务网络难以实现灵活的业务组合，难以为用户提供个性化、综合化服务；业务网易受到攻击，溯源能力不足，存在安全性隐患；业务网与承载网适配性较差、系统效率低、灵活性差；用户数据分离或关联关系复杂；多业务平台没有实现统一的 SP/CP 接入，没有开放的、便利的业务开发环境，导致第三方应用逻辑和内容资源难以重用；各增值业务平台的业务能力均比较单调，没有统一的业务管理平台来融合管理多种业务能力。此外，现有网络的运行与维护体系严重滞后于承载网络和业务网络的发展。

### 3. 有线电视网的问题

有线电视网是国家信息基础设施的重要组成部分，但是当前其单向的推送式服务形式和单一的盈利模式已经不能满足人们对多种娱乐方式的需求，其正面临着向数字化过渡、双向化改造、扩展信息服务能力和更新商业模式的艰巨任务。

对于数字化改造的问题，在跨越了“改造还是不改造”的争议门槛后，现今面临的主要问题是“如何改、怎么改”的问题。传统的模拟电视网向数字化转换的战略在我国已经全面展开，在逐步摸索的过程中，形成了“青岛模式”、“杭州模式”、“深圳模式”等多种发展模式，目前国家正逐步推进有线电视数字化由部分城市试点向全国大中城市全面铺开。同时按照大容量、双向交互、多功能的要求大力推进网络改造，积极拓展网络业务和服务，推动数字有线电视全功能网的建设。

## 5.4.2　国际研究现状与趋势

网络体系结构是个笼统的概念，不同研究背景和研究目的的科研人员对其具体的研究范畴有着不同的理解。但是一般认为网络体系结构主要包括功能模型、拓扑模型和应用模型等，其中功能模型是核心部分。功能模型定义网络系统如何被分割成小的、具有不同功能的部分，以及这些部分之间如何相互作用，如何通过这些部分的排列组合来实现网络系统整体的功能。

目前国际上对这一领域的研究可以分为两部分：一部分从网络基础理论研究的角度出发来试图解决新型网络的基本科学问题；另一部分从工程技术研究的角度出发解决网络与业务实现的具体问题。这两部分是相互影响、互动发展的。目前，在新型网络体系结构的基础理论研究中有两个重要的方向：一个是对现有网络层次化功能模型的改进；另一个是探索非层次化的网络体系结构。

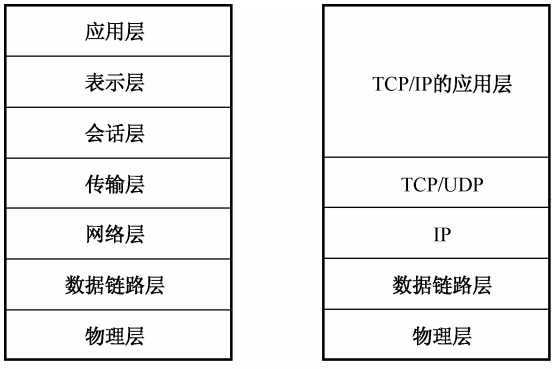
### 1．层次化功能模型的改进

现有层次化功能模型的改进有两个重要趋势：一个是层次模型的简化，也就是网络层次的扁平化趋势；另一个是层次化模型中的跨层访问和多层迭代。

（1）网络层次的扁平化趋势

通信网络层次化功能模型的提出是通信领域里程碑式的技术突破，ISO 的 OSI 七层协议栈模型、互联网的 TCP/IP 四层协议栈模型、ITU-T X.200 的层次化模型（X.200 采用了 OSI 模型，并从 ITU-T 角度对其概念进行了重新规范，成为一种广泛应用的网络模型和网络设计方法）改变了传统电信网中网络与业务不分离的局面，把业务实现方式从具体网络技术中解放出来，促进了综合业务的繁荣，直接推动了电信网和互联网的快速发展，促进了社会信息化进程。

OSI 模型/X.200 模型和 TCP/IP 模型如图 5-12 所示。




（a）OSI模型/X.200模型　　（b）TCP/IP模型

图 5-12　OSI 模型/X.200 模型和 TCP/IP 模型

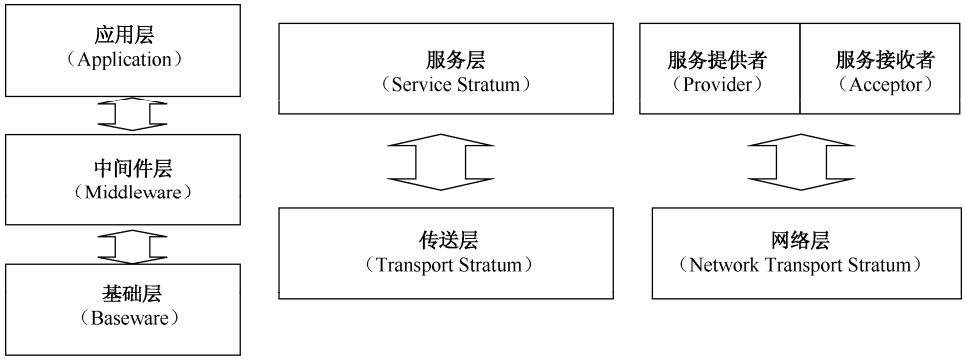
但是随着网络规模和用户规模的扩大，以及新业务需求的不断提出，尤其是三网融合发展方向的确立，传统的层次化功能也日益暴露出越来越多的缺陷和不足。

首先，过多的网络层次意味着需要定义复杂的功能接口，增加了网络协议和系统实现的复杂性，降低了系统工作效率；其次，多层之间存在着层间功能重叠、功能划分不清、层次固定难于扩展的问题。业界对这些问题的反思使得网络层次扁平化成为重要的研究趋势。但是对于网络层次如何简化有不同的研究成果。

目前由 ITU-T Y.130 定义的信息通信结构（ICA，Information Communication Architecture）代表的是“Information Communication”领域内一种标志性网络技术的结构进化，把未来网络划分为三层结构，即应用层（Application）、中间件（Middleware）层和基础（Baseware）层，把“中间件层”和“基础层”都划入基础设施范畴。

ITU-T 的 NGN 模型中，网络层次已经简化为两层：业务层（以 IMS 为主）和传送层（目前正在启动未来包交换网络 FPBN 的研究）。麻省理工学院提出的 FARA（Forwarding Directive，Association，and Rendezvous Architecture）模型中也对网络层次进行了简化，推荐了二层的网络结构。定位为提供多媒体服务的下一代网络的平台——流媒体宽带网（MP，Medianet Protocol）也将网络分为两个层次：网络层和媒体层。

典型结构模型如图 5-13 所示。




（a）ICA结构模型　（b）ITU-T的NGN结构模型　（c）MP技术网络结构模型

图 5-13　典型结构模型

（2）网络层次的迭代

随着网络技术的增多和网络设备更新换代速度的加快，在实际的网络建设中出现了多个网络层次的迭代，如 IP over MPLS over IP over ATM over SDH over DWM 等，原有的较为清晰的层次迭代关系变得复杂。多层迭代需要每个层面都能够具有对其他层次的统一的功能接口，而不是原来 ISO 的 OSI 七层模型中下层只为其相邻的上层提供接口。因此出现了支持跨层访问的层次化网络模型。

跨层模型的主要目标是：通过定义一个灵活的、可扩展的网络体系结构，实现各个网络层次的集成，建立一种灵活的网络资源感知、分析、决策、调度的新模式，从而改变传统层次化网络模型中一个网络层次只能与其直接相邻的网络层次交换信息、缺少相关性分析和综合决策机制、缺乏各层资源综合利用的局面，给网络以更大的灵活性和扩展性。

但是这种跨层模型对每个网络层次的设计提出了更高的要求，要求规范每个网络层次的输入和输出的信息格式和调用函数，只有每个网络层次对外的接口是统一模式的，才能实现各个网络层次的跨层直接访问和调用。这些统一的对外接口实际上形成了一条逻辑总线(而不是一般功能模型中的两条总线：输入总线和输出总线)，各个网络层次都是插在这个逻辑总线上的，因此每个网络层次可以通过总线来调用其他网络层次的功能模块，从而实现多个网络层次的灵活调用和组合。

跨层访问模型如图 5-14 所示。

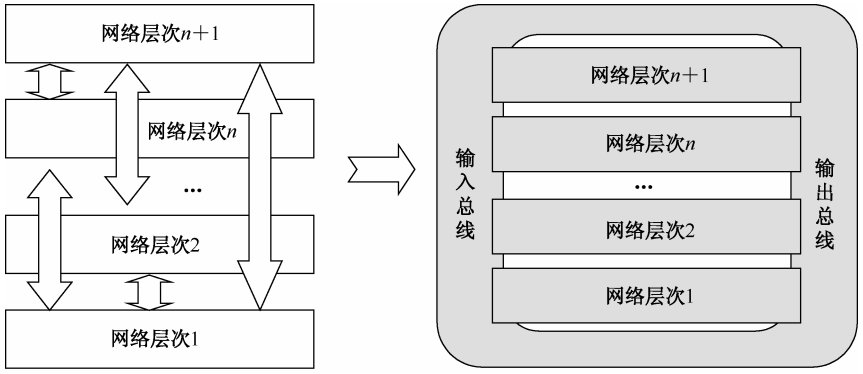



图 5-14　跨层访问模型

跨层直接访问模式实际上打破了传统层次模型中的层次相邻关系，每个网络层次有更大的自主性，可以支持更加灵活的网络层次迭代，为此 ITU-T 提出了一套新型网络设计与分析方法，见 ITU-T G.805 和 G.809。在 G.805 和 G.809 中，网络层次的通信模式被抽象为“面向连接”和“无连接”两种，把不同网络层次之间的迭代关系转化为面向连接的分组交换（CO-PS）与面向无连接分组交换（CL-PS）之间的耦合迭代关系。

### 2．非层次化网络体系结构

ITU-T G.805 和 G.809 实际上反映了一种网络设计的新思路，通过对功能模块的提炼和灵活组合来实现更加有扩展性的网络体系结构，只不过 G.805 和 G.809 所凝练的功能模块是面向连接的分组交换（CO-PS）与面向无连接分组交换（CL-PS）的，还是保留了层次化模型。随着这种研究思路的深入发展，很自然地出现了其他功能

模块的提炼方法和组合方式，也就出现了一些打破层次化结构的、新型的非层次化网络体系结构，其中比较有代表性的有面向对象的网络体系结构、基于角色的网络体系结构、服务元网络体系结构等理论模型等。

多层迭代模型如图 5-15 所示。

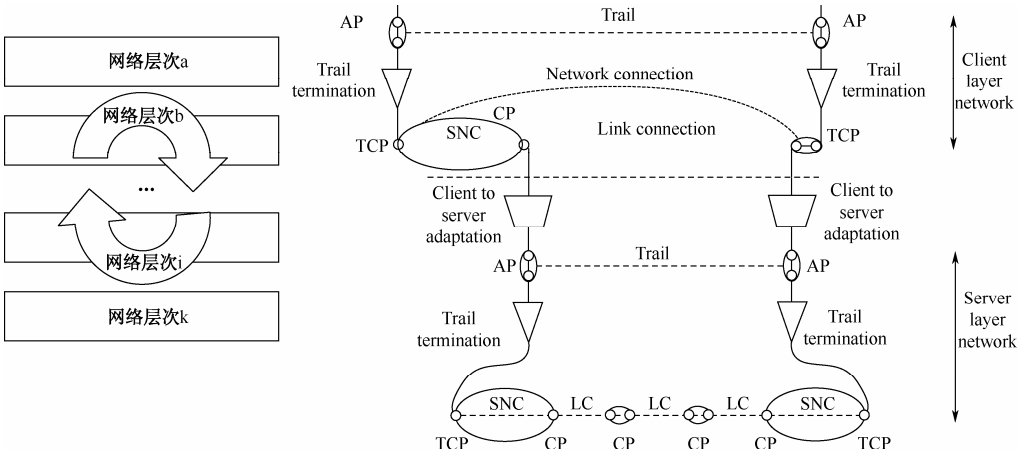



图 5-15　多层迭代模型

### 3. 网络体系结构

（1）面向对象（Object Oriented）的网络体系结构

面向对象的网络体系结构：这种新的网络体系结构采用计算机领域的面向对象技术，通过功能聚合与抽象，定义了多个功能“类”（Class），形成了工具箱，这些工具箱中的工具（网络功能模块）可以灵活组合，实现更加灵活的网络功能。这些类可以“派生”出各种满足特殊需要的工具；通过类的实例化可以满足个性化特定需求。

面向对象（Object Oriented）的网络体系结构如图 5-16 所示。

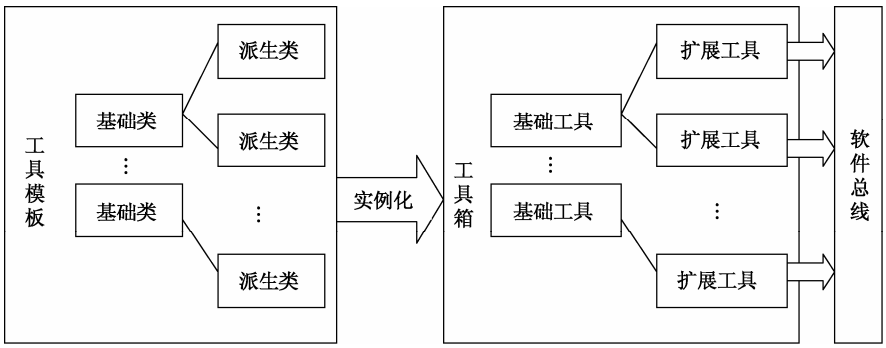



图 5-16　面向对象（Object Oriented）的网络体系结构

目前这个方向的研究还处于初级阶段，研究重点包括工具箱的定义（网络功能的抽象与封装）与工具的组合交互模式（总线结构与调用方式），工具不同的组合方式与协作工作方式对应不同的新型网络。目前这个方向只提出了一种网络设计与实现思路，并没有具体的网络设计实例。

（2）基于服务元（Service Unit Based）的网络体系结构

基于服务元的网络体系结构：针对现有的分层网络体系结构存在的层间功能重叠和复杂的分层处理过程所带来的网络服务效率低下的问题，服务元模型改变了层次模型中层次间的服务与被服务关系，它通过将网络服务功能拆分为服务元，由服务元构成服务团队，再由服务团队向应用群提供服务。服务元只提供服务，不接受服务，避免了层间交互和服务传递的开销。服务元不仅能为本节点应用提供服务，而且不同节点的服务元可以合作向某一节点或整个网络提供服务。实际上每个服务元就是一个具有一致输入/输出接口的单独功能模块，能够完成一项或多项独立的工作。服务元是能够提供网络服务而又隐藏内部细节的最小实体。

基于这种网络体系结构所建立的网络是端到端的虚电路结构，同样的源、目节点地址因服务类型（实时音、视频或文本数据和优先级等）的不同而选用不同的服务元、构建不同的虚电路来传送，保证了服务质量和安全。我国曾经在 973 计划中支持过这个研究方向。

（3）基于角色（Role Based）的网络体系结构

基于角色的网络体系结构：2002 年 Braden 等人在其文章 *From protocol stack to protocol heap-role-based architecture* 中提出了无层次的基于角色的网络体系结构设计思想。通过明确信息通信过程中的实体（主体）和其在通信过程中所扮演的角色，把通信过程转化为多个角色主体之间协作工作的过程。基于角色的网络体系结构从角色及其合作的角度分析了面向角色的工作模型、设计方法。

基于角色的网络体系结构是一种通用的体系结构，包含了多种网络体系结构。近两年出现的一种新的互联网体系结构 I3（Internet Indirection Infrastructure），以及由它进行扩展后的 Secure-I3 和结合了 HIP 技术的 Hi3 就属于基于角色的网络体系结构。I3 是加州伯克利大学的 Ion Stoica 等人提出的一种结合 P2P 技术、用于转发分组的应用层跨层网络。I3 是一种打破了现有互联网端到端通信模式的体系结构，将“indirect”引入了通信机制当中。通过 indirect 机制，将核心网的功能发挥出来。I3 中的主要角色有三种：信息发送者、信息接收者和信息传递者（trigger）。目前，网络分组的发送和接收是一个统一的过程，源端发送分组意味着目的端在正常情况下会接收到分组。而在 I3 中，发送和接收是两个独立的过程，接收方告知 I3 自己的位置，以及所需分组应该具有的数据特征，I3 就可以将具有该特征的分组转发给接收方。同样，发送方并不需要指定分组的接收方，而只需要标记分组的数据特征并将

分组交给 I3 即可。由于发送方根本不需要知道接收方的身份和位置，因此只要移动节点及时向 I3 更新自己的位置信息就可以保证正确地收到分组。对于一个用户群来说，只要每个用户告知 I3 相同的数据特征，它们就可以收到相同的分组。因此，I3 能够很自然地支持主机移动和组播。例如，接收者（主机 R）在 I3 体系中插入一个 trigger（id，R），那么主机 R 就可以接收所有具有标识符 id 的数据包，基于角色的网络体系结构如图 5-17 所示。

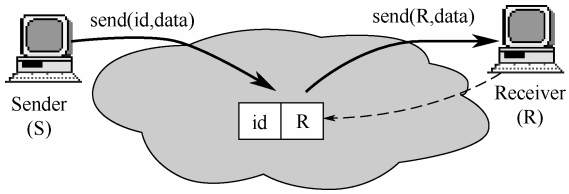



图 5-17　基于角色的网络体系结构

由于 trigger 的出现，可以实现受限路由，如在 trigger（id，R）中 id 可以为一个序列，{id1，id2，id3}从而支持数据包在 id1，id2，id3 之间的顺序传递。I3 也可以从体系结构上支持主机的移动性。

另外，由留美华人技术人员提出的宽带多媒体网络 MP（Medianet Protocol）技术也可以看作一种基于角色的新型网络体系结构，其面向视频通信业务，把网络角色划分为“接收者”、“发送者”和“储存者”，并且基于角色来设计网络功能模型和组网模型，支持广播、组播、点播和媒体节目调度功能，具体如图 5-18 所示。

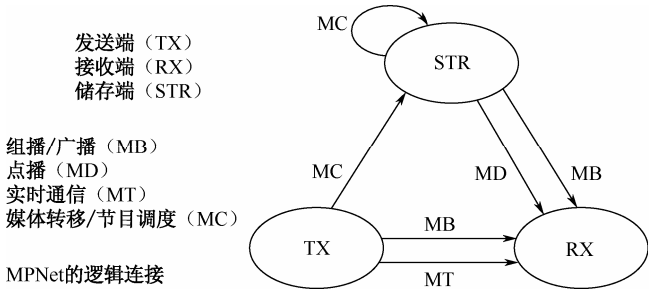



图 5-18　宽带各媒体网络 MP 技术

### 4. 趋势展望

基于上述分析，目前新型网络体系结构的研究正向着扁平化、多层迭代、功能灵活布置的方向发展。这些发展方向不是孤立的或相互排斥的，而是逐步融合的。

在未来网络体系结构的研究中，层次化模型依然有着重要的指导意义，但是基于角色、面向对象等非层次化网络体系结构的设计思路要发挥越来越重要的作用。

这几种网络体系结构的研究方向需要进一步融合。

在设计一个新型网络体系结构时，可以不必沿袭传统层次化网络模型的设计方法，而是分别针对承载网和业务网络，从应用场景出发，明确通信中的角色（Role based）及这些不同角色之间的协同关系，构建角色模型；在此基础上明确这些角色协同工作时需要涉及哪些必要的功能，从而构建“工具箱”。这些工具箱中的功能模块的不同组合方式对应不同的网络体系结构。甚至可以进一步研究这些工具协同工作的总线结构（或其他可能的工具组装方式），从而实现新型网络体系结构的通用设计平台，在这一平台上可以更加灵活地设计新型网络。

例如，在新型承载网络的设计中，可以不必先划分网络层与链路层，分层单独进行设计，而是把承载网中所设计的角色、通信需求明确以后，先规划新型承载网应该包括哪些功能模块，这些功能模块中哪些是基础模块、哪些是衍生模块，规范各个模块的外部接口（功能模块的具体实现有多种方式，如面向对象方法，但是这属于工程实现技术，是一种具体的网络功能设计方法）。在此基础上，可以设计多种功能模块的组合方式（单独的功能插件可以组合成紧密结合的大颗粒的功能实体——“功能片”）和工作流程，从而实现更加灵活、开放的网络体系结构。

三网融合趋势下的业务网络设计也可以采用这种思路，即先明确各种业务的通信角色（在新型业务体系研究中要着重面向视频类业务，因为视频类业务是未来通信的主要方式），再精炼、抽象、聚合出功能集合，共性的部分可以成为基础工具，并可以基于此派生出针对特定业务的扩展工具，从而通过这些功能模块的不同组合实现针对特定业务的新型业务体系。

因此，角色、面向对象等技术可以作为设计新型网络体系结构的有效手段，并与层次化网络体系结构相结合。而在层次模型中，充分考虑到网络与业务过度分离所带来的诸多问题（如资源感知困难、跨层资源管理能力弱、网络管控能力较差、网络与业务匹配效率低下、商业模式不合理等问题），可能会出现新的网络层次——网络层、感知与黏合层（见图 5-19），这个新的网络层次可以在网络与业务分离的趋势下更好地实现网络与业务的匹配，提高资源利用率和工作效率，同时此层还负责构建统一的网络边界，实现 UNI/NNI/SNI 接口，实现各种异构网络的统一接入和标识转换（映射）。

因此，在未来网络体系结构研究中，以下几个领域可能会成为新的研究热点：① 网络及业务的感知与黏合模型与具体技术研究，这是一个创新的热点；② 工具箱的设计，即网络功能与业务功能的抽象与封装，这是设计要点，面向对象技术可能发挥重要作用；③ 功能片的组成，即网络功能和业务功能的组合方式与工作流程，基于角色的设计方法成为功能片设计的重要手段。

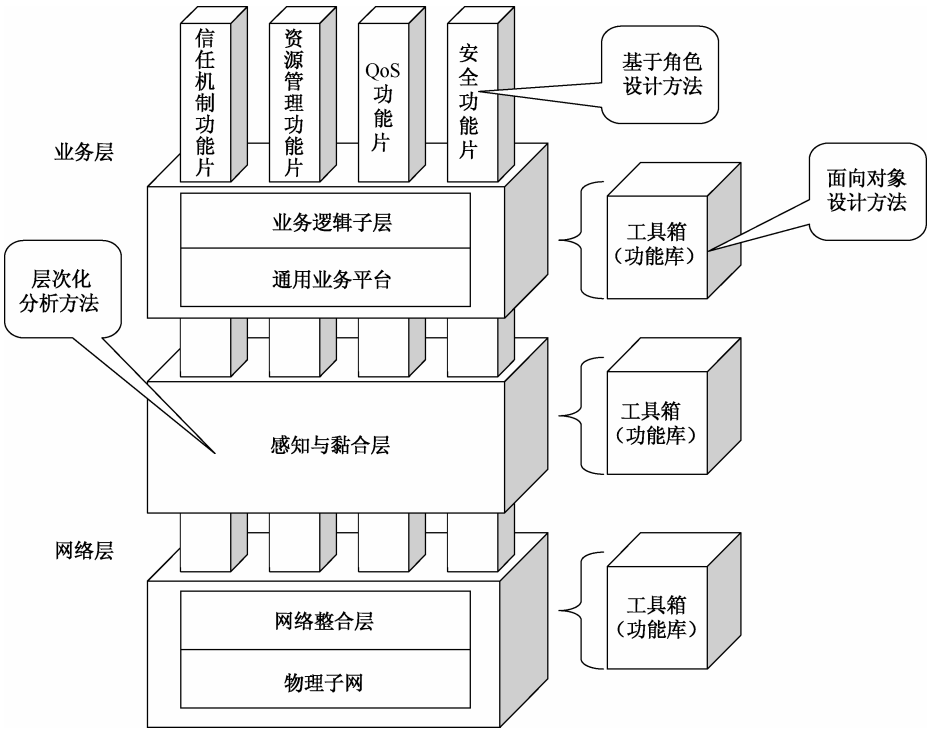



图 5-19　新的网络层次

## 5.4.3　中国研究现状

我国高度重视未来网络研究和试验工作，“十二五”期间，863 计划安排了“未来网络体系结构创新环境 FINE”、“软件定义网络（SDN）关键技术研发与示范”项目。国家发改委 2012 年设立 CNGI 新型网络体系结构技术研发与试验项目，包括“地址驱动的新型网络体系结构、技术研发和试验”、“可演进的下一代高智能网络架构研究和试验”等。973 计划也已经支持多项未来网络的基础研究。

**1. 我国未来网络研究在理论基础创新、国际标准、产业示范应用等领域取得了大量成果，提出了一批新型网络体系架构的解决方案，形成了多个有实力的科研队伍**

工信部电信研究院提出的“公共分组数据网 PTDN”，保留现有 IP 网络的所有技术优势，并面向未来网络需求，解决现有 IP 网络问题，是由我国掌握关键技术的未来网络解决方案。目前 PTDN 已主导系列国际电联标准，建成国内领先的规模实验网平台，并研发出面向商用的 PTDN 设备，初步奠定了 PTDN 产业链的发展基础。目前 PTDN 正在军网和中石油等行业专网中开展应用试点。

北方交通大学提出了“一体化可信网络与普适服务”架构，定义了包括一体化可信网络与普适服务的两层体系结构模型，该网络原型系统在 2009 年 12 月通过科技成果鉴定，相关专利已转让给了中兴公司，中兴公司正融合这个技术方案研发自己的网络解决方案。

中科院提出了“层次化交换网络”，目标是构建一个高性能、可管理、可控制的下一代互联网。目前这个技术方案更多地侧重于理论研究与原理性验证，尚未实际应用。

此外，解放军信息工程大学提出的“可重构网络”及中科院的“SOFIA”项目，从新型网络架构、路由、编址、安全和网络虚拟化等方面进行了未来网络研究和探索，形成了一系列研究成果，对互联网的移动性、安全性、可管、可控等方面进行了改进。

**2. 我国未来网络研究的主要技术方向基本覆盖国际上的主流技术方向，但是研究深度普遍不足，原创技术较少**

我国未来网络研究目前研究涵盖了标识体系（标识与地址分离、边缘与核心分离等）、网络可重构、控制与转发分离、网络转发集成存储与计算能力等主要技术方向，但是以跟随为主，自主创新较少或缺乏影响力。虽然在技术点的研究方向上基本覆盖，但是在未来网络技术创新试验环境建设方面起步较晚，总体落后。我国尚未建成与美国 GENI、欧盟 FIRE 类似的大规模未来网络实验床，不利于科研领域的开放、协作和创新，不利于研究成果的验证和产业转化。

从国际上未来互联网研究的趋势来看，网络创新环境，或称为试验床，是推动未来网络技术研究的重要手段。我国也应重视未来网络创新环境的建设，一方面支持面向核心架构创新的专用试验床；另一方面整合既有的试验床，通过联邦方式建立可持续演进的未来网络实验环境。同时，在试验床的建设之中，应具有更长远的战略视野，考虑试验环境成为未来新一代互联网 tier1 的可能性，通过与国外现有平台的互通扩大国际影响。

## 5.5　未来网络试验平台

### 5.5.1　发展未来网络成为欧美等发达国家的战略取向

未来互联网技术目前还处于发展初期，各种技术层出不穷，技术特点纷呈，这正是技术创新的活跃期和高峰期，这一轮的技术创新不仅会直接影响全球互联网未来数十年的技术走向，而且由于互联网作为全球信息基础设施的重要地位的凸显，

其对未来信息社会的政治、经济、文化、生产生活等各个领域都会产生长期而深远的影响。

在技术创新活跃期，应该建立某种机制和环境来保持和鼓励未来互联网的技术创新，美国、欧盟均结合各自在 ICT 领域的总体战略，十分重视未来互联网创新实验环境的构建。

#### 1. 美国的战略考虑

美国凭借其在互联网领域的先发优势，从 20 世纪 80 年代至今一直占据着全球信息通信领导者的地位。在全球信息通信技术变革和产业融合转型的关键时期，尤其是在应对全球金融危机的重要关头，美国期望通过未来互联网创新实验环境的构建，来促进信息通信的技术创新和业务创新，构建新型国家信息基础设施，继续引领全球 ICT 技术方向和产业发展，继续保持其在未来信息社会的技术和产业制高点、ICT 领域的全球领导地位。发展未来互联网是其国家 ICT 发展总体战略的重要组成部分。

#### 2. 欧盟的战略考虑

欧盟期望在全球宽带发展提速的大背景下，能够在自身无线和移动通信发展具备较大优势的基础之上，将下一轮宽带的发展与移动互联网等紧密结合起来，逐步摆脱在现有互联网发展格局中一直以来欧盟对美国的跟随态势，从而实现欧盟在全球互联网领域对美国的超越，并能够最终奠定欧盟在全球互联网领域的领先地位。

### 5.5.2 构建未来网络创新实验环境成为欧美发展未来互联网的重要举措

在发展未来互联网的总体战略取向下，美国和欧盟都把构建未来网络创新实验环境作为落实未来互联网发展战略的重要举措。纷纷构建各自的未来互联网创新实验平台。其基本出发点有以下几点考虑。

① 通过未来网络创新实验平台来为各种创新性技术提供规模化的、综合实验环境，使得各种未来网络创新架构和关键技术均能够得到充分的实验和验证，保持未来网络的技术创新和业务创新活力。从中孕育出主导性的技术点、融合并催生出未来网络的核心技术方案，从而把未来网络创新实验平台构建为未来网络技术的“孵化器”。

② 欧美的未来网络创新实验平台均是对外开放的，支持并鼓励其他国家科研单位甚至个人参加，通过这种方式把全球创新的思路和技术吸纳到其创新实验平台中去，从而把未来网络创新实验平台构建为吸纳全球智慧的“智库”。

③ 未来互联网不会凭空产生和构建，欧美重视未来网络创新实验平台的建设隐

含着有将其发展成为未来互联网雏形的想法，欧美的未来网络创新实验平台可以成为未来互联网演进的起点（1969 年美国 ARPANET 的构建就是一个成功的先例）。因此欧美未来网络创新实验平台的整体架构和布局可能对未来互联网全球网络架构有着直接的影响，按照目前的发展趋势，欧美将有可能继续保持未来网络联网中 tier1 的优势地位。

## 5.5.3　欧美的未来网络实验环境包括四大类、三个层次的实验床

欧美在具体构建未来网络实验环境的设计原则、建设方式和发展思路等方面具有很强的相似性。

### 1. 欧美均把构建开放协同的试验床的联邦作为基本的设计原则

欧盟在建设其未来网络实验环境——FIRE（未来互联网研究与实验环境）时，本着一个基本的设计与建设原则：构建各类实验床的开放、协同的联邦（Open Coordinated Federation of Testbeds）。

美国在其 GENI 计划的 SPIRAL2 阶段提出构建开放的联邦模式的、能够融合 SPIRAL1 阶段各种实验床的综合实验环境，明确传达出了构建开放协同的试验床联邦的意图。并且这种意图在其正在实施的 GENI 技术的 SPIRAL3 阶段得到更充分的重视和更具体的落实。

### 2. 欧美出于不同的实验目的构建了四类实验床

美国和欧盟构建的未来网络实验床不是单一的一个床，而是同时支持众多实验床的建设，这些试验床归纳起来可以分为四类。

（1）针对特定应用的专用试验床

例如，美国的 GENICloud 是为了专门实验云计算技术方案的；欧盟的 VITAL++ 是专门用于实验 IMS+P2P 技术方案的，欧盟的 WISEBED 是用于实验传感器网络的，CREW 是用于实验认知无线电等频谱优化技术的。

（2）基于可编程技术的试验床

例如，美国的 Enterprise GENI 主要是利用 Openflow 技术来构建可重构的实验床的；欧盟的 OFELIA 项目也是利用 Openflow 技术来构建可以对更底层的创新性技术进行实验的实验床的。

（3）基于可重叠技术的试验床

例如，美国的 PlanetLab 与 PlanetLab2 及欧盟的 OneLab 和 OneLab2 都利用 P2P 等跨层技术来构建更加通用的、可以同时实验多种技术方案的实验床。但是这些试验床通常很难支撑对底层技术的创新性实验，主要用于实验创新性的业务与应用。

（4）联邦模式的试验床

例如，美国的 CMULab 和欧盟的 PII 项目都研究如何通过联邦方式把现有的试验床及正在建设的实验床进行集成，实现这些专用床和通用床的长期持续发展。

联邦模式的试验床如图 5-20 所示。

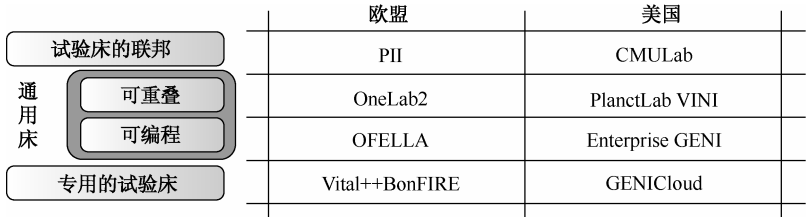



图 5-20　联邦模式的试验床

**3. 这四类床可以按照其可以实验的技术方案的革命性分为三个层次**

第一层：专用床。优点：可以实验编址、命名、路由等更加核心的未来网络技术方案，这些技术方案通常需要特定的、其他技术方案不用的基础设施和关键机制。缺点：只实现对特定技术方案的、短期的实验，这些试验床的规模通常有限，而且开放性不高。

第二层：通用床。优点：可以对多种技术方案进行并行设计，可以降低试验床建设成本和使用门槛。缺点：有限于通用床所采用的基础技术和核心基础设施，只能对一些 L4～L7 层的技术方案进行实验，不支持对 L2～L3 层技术方案的实验。

第三层：联邦床。优点：可以对一些出于短期实验目的的专用床的资源进行整合和再利用，可以实现多个独立床之间资源的共享与优势互补。缺点：与通用床的缺点类似，也是难以支持对编址路由等核心技术的实验。

## 5.5.4　欧美未来网络实验环境的建设兼顾两大趋势

基于对欧美四类试验床的技术特点的分析，未来网络实验环境的建设明显地表现出两大趋势。

### 1. 趋势一：创新架构需要专用试验平台

通过建立专用试验平台（见图 5-21）来对底层核心技术进行实验，从而推动未来互联网基础架构的革新。

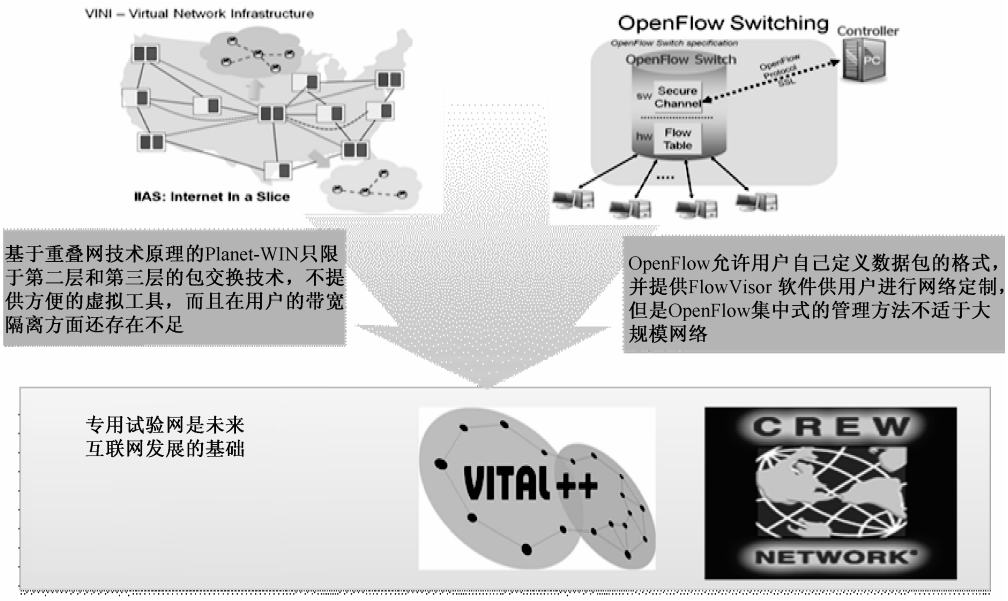



图 5-21　专用试验平台

目前欧盟在 FP7 中支持了众多专用实验环境的建设，如 BONFIRE 用来实验云计算技术；SMARTSANTANDER 用来实验传感器网络的物联网技术；CONNECT 用来实验多种无线技术的融合接入技术；CONVERGENCE 用来实验以内容为中心的订阅/发布模式的网络新技术；EULER 用来实验分布动态路由新机制；HOBNET 用来实验绿色节能网络新技术；LAWA 用来实验大规模数据分析与挖掘技术等。

### 2. 趋势二：联邦是试验床发展的方向

通过构建各类实验床的联邦（见图 5-22）来提高资源的使用效率，解决专用网的再次使用问题；扩大试验规模，可以协同完成单个床不能完成的试验。

试验床的联邦包括两种建设模式：一种是中央与地方分权的联邦模式，称为 CENTRAL 模型；另一种是对等联合的联邦模型，称为 DISTRIBUTED 模型。

每个专用实验床和通用实验床都可以利用某种资源整合技术抽象为各类资源 Resource（R）、域管理器 Domain manager（M）、资源元数据注册管理服务器 Registry（Reg）和资源操作集合（SET），见图 5-23。

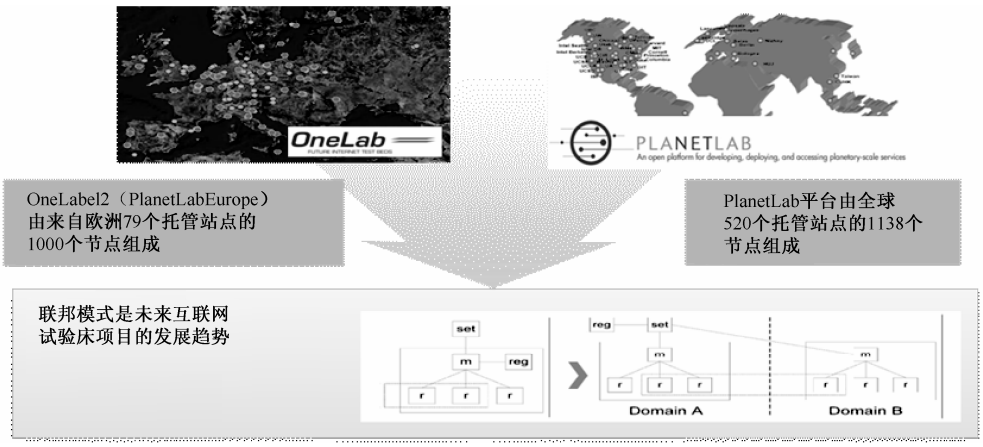



图 5-22　试验床的联邦

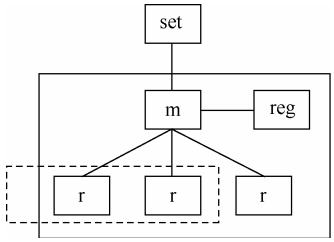



图 5-23　资源的抽象

CENTRAL 模型的工作方式如图 5-24 所示。

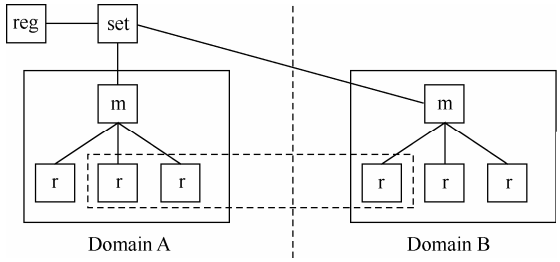



图 5-24　CENTRAL 模型的工作方式

每个试验床把各自的资源进行整合与抽象，并把各自的资源注册到统一的资源元数据管理服务器 Reg 中，通过 Set 实现对不同实验床资源的统一管理与利用。

DISTRIBUTED 模型的工作方式如图 5-25 所示。

每个实验床均把各自的资源进行整合与抽象，通过与其他试验床之间的某种协议实现对其他试验床资源的调用——“借用”。

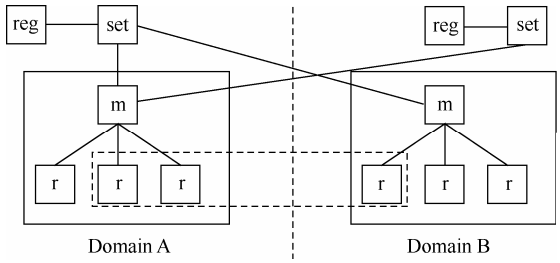



图 5-25　DISTRIBUTED 模型的工作方式

目前这两种联邦模式在欧盟的 FP7 中均在进行研究，并且已经出现了一些用于联邦目的的基础协议，如 SFA（Slice Federation Architecture）及其相关协议。目前美国的 PLANETLAB 和欧盟的 ONELAB 均支持 SFA 架构，已可以实现互联。

## 5.5.5　我国在未来网络试验环境建设的重点

抓紧构建我国未来网络创新实验环境，催生技术与业务创新。

① 支持面向核心架构创新的专用试验床。支持国内有一定技术与实验基础的层次化网络、未来分组交换网络（FPBN）、普适网络等创新性网络体系结构的实验床建设。

② 整合既有 Testbed，通过联邦方式建立可持续演进的未来网络实验环境。利用联邦方式，整合国内既有试验资源，形成长效实验环境；支持具有 20 个左右节点的创新型网络实验网，为网络的新协议、新体系提供演示验证环境；对多个“床”的整合，需要政府发挥重要作用。

③ 试验环境一定要与国外现有平台互通，扩大国际影响。考虑试验环境成为未来新一代互联网 tier1 的可能性，实现与 FIRE 和 GENI 的对接，将试验环境和专项项目对外开放。

# 第 6 章 典型未来网络技术方案

## 本章要点

- ✓ SDN（Software Defined Networking）
- ✓ NDN（Named Data Networking）
- ✓ NEBULA
- ✓ XIA（eXpressive Internet Architecture）

## 本章导读

美国在 20 世纪初就开始了未来网络领域的战略布局，持续资助未来网络技术研究，美国自然科学基金会（NSF）相继启动了 GENI 计划、FIND 行动、FIA 项目等。目前美国未来网络技术研究全球领先，对全球未来网络技术走向有着重要的影响。

### 1. 美国在未来网络领域的战略意图日渐清晰

美国凭借其在互联网领域的先发优势，自 20 世纪 80 年代至今一直占据着全球信息通信领导者的地位。在互联网演进过程中，美国坚持“两条腿走路”，一方面希望通过维护现有互联网治理格局、坚持现有互联网技术体系，来继续巩固和强化其在现有互联网领域的超霸地位；另一方面，美国也充分认识到现有互联网存在的突出问题，以及来自欧盟和亚太等国家发展未来网络的竞争压力，加紧未来网络的超前布局，强化未来网络技术创新与试验，希望将现有优势延续到互联网的长期演进中。

### 2. 美国在未来网络领域的战略重点较为突出

近几年，美国不断完善其未来网络战略部署，形成了五个方面的战略重点和相应的技术方向。

（1）通过未来网络技术创新来释放网络活力，推动经济发展。美国将网络技术创新与产业变革紧密结合，通过网络技术创新打破目前相对封闭的基础通信网络，向互联网应用开放更多网络状态信息和网络控制能力，释放互联网更大的创新活力，催生新的产业层次和业务模式，支持互联网企业在网络经济发展和产业变革中发挥主体作用。基于这一战略考虑，美国在项目设置上支持开放流表（Open Flow）、软件定义网络（SDN）等技术的研发，通过将网络的控制层与转发层分离，实现网络向应用开放更多控制权，支持应用按需定制网络。网络控制权的开放，一方面可为互联网企业利用传统网络运营商的基础网络来构建满足自身需求的廉价高效网络提供可能，促进云计算、物联网等业务的创新发展；另一方面可为传统电信企业构建智能管道提供技术途径，为网络运营商转型发展创造机会。

（2）通过未来网络技术创新来完善互联网应用基础设施，提升网络能力。随着视频等大数据量业务的发展，以内容分发、流量优化为典型特征的互联网应用基础设施越来越受到美国政府的重视。相关的科研项目成为美国政府支持的重点，如名字定义的网络（NDN）、间接互联网架构（I3）等项目，这些项目通过内容路由实现以内容为中心的网络，在网络架构中集成计算、存储、分发等能力，在互联网的网络层与应用层之间形成以内容为核心的“应用基础设施层”，从而细化互联网产业链，

提升互联网的内容分发能力，大幅改善用户体验。

（3）通过未来网络技术创新来支持互联网向太空及外太空发展。美国面向太空及外太空控制权的争夺，加快符合星球间大时延、高损耗等通信条件的空间互联网技术研发，支持地空互连、卫星（太空飞行器）互连，支持网络向外层空间发展。目前美国已主导完成了太空互联网技术标准，组织开展了太空互联网的技术试验，在太空互联网领域初步形成了先发优势。

（4）通过未来网络技术创新来强化网络安全机制，服务国家安全。考虑到互联网安全可信架构的缺失与维护国家安全和保护个人隐私需求之间的矛盾日益突出，美国将网络技术创新与国家安全紧密结合，通过在网络中内嵌安全机制来提高基础网络的安全保障能力和水平。一方面，美国试图通过对通信实体数字签名、在网络架构中增加新的网络安全子层来实现内嵌安全机制，以改变目前外挂式的网络安全机制，从体系结构上保证网络的安全性。另一方面，美国投资实施“影子网络”计划，利用无线自组织网络技术开辟海外渗透新战线。例如，支持构建“行李箱互联网”和“影子手机通信网”，把“行李箱”作为控制中心，将手机等终端组织成一张无线网络，用于间谍活动和组织串联。

（5）高度重视未来网络技术试验，形成先发优势，掌控未来网络。考虑到未来网络技术处于创新活跃期，为避免技术“押宝”的风险，美国在重视未来网络技术创新的同时，极其重视“未来网络试验床”的建设，培养未来网络技术创新的“土壤”。未来网络试验床利用统一的网络操作系统，通过联邦方式来整合现有各类网络资源，为多种网络技术方案提供并行试验的环境，鼓励各种网络技术在试验床上共存与竞争。最终胜出的未来网络技术方案将以试验床为网络核心层（Tier1），并实现与现网的互通与融合，从而复制 ARPA 网络演进为现有互联网的成功经验和模式，孵化未来网络雏形，进而掌控未来网络。目前，美国通过 GENI 计划整合了既有的 Internet2、PlantLab 等试验网络，建成了覆盖全球五十多个网络、数千个网络节点、互相连通的未来网络试验床，吸纳了众多网络技术方案，在战略布局中已经形成了先发优势。

### 3. 未来网络技术快速创新，一些成果已开始应用

除美国以外，欧盟和亚太也纷纷瞄准互联网技术变革带来的难得历史机遇，加强未来网络技术创新与试验，争夺网络空间基础设施的主导权。综合全球未来网络技术发展情况来看，研究形成国际公认、技术体系完整的未来网络体系架构是一项长期而艰巨的工作，可能需要 20 年左右的时间。但是未来网络研究可以形成“新技术池”，其中一些技术点可以与现网结合，能够在较短时间内对现网演进产生重要影响。目前，在未来网络研究中，网络的控制与转发分离、标识与地址分离、发送与接收分离等成为重要的技术方向和思路。其中，美国在 GENI 计划中支持 Openflow

技术研发，催生了软件定义网络技术（SDN）。目前 SDN 技术已经开始产业化，2012 年谷歌在其内部骨干网络中规模应用，腾讯、中国移动等也开始了相应的组网试验，预计在未来 2～3 年，SDN 设备将会在现网中实现规模应用。

# 6.1 SDN（Software Defined Networking）

当前，软件定义网络（SDN）成为业界相当时髦的一个话题，SDN 技术及其可能带来的影响受到了学术界和产业界的高度重视，但是不同研究背景的专家由于各自关注点和知识结构的差异，对 SDN 有着不同的理解和认识，本节试图从 SDN 技术发展脉络的梳理入手，分析 SDN 技术的内涵、本质特征、应用领域、发展趋势，进而分析判断 SDN 技术发展带来的影响。

## 6.1.1 “众说纷纭”SDN

通过参加网上论坛、技术研讨会、标准讨论会等，可以发现目前对 SDN 关注度比较高的专家大致可以分为三类：IDC 设计与运维人员、数据设备设计研发人员、未来网络研究与试验人员。这三类专家关注 SDN 的出发点并不相同，对 SDN 的认识也不一样，对 SDN 的发展愿景和期待也各不相同。这些专家坐在一起，虽然表面上都在讨论“SDN”，但是各自心中理解的 SDN 存在较大差异，通常“各说各话”。

一项新技术出现以后，一些专家热衷于追溯这个概念最早是谁提出来的、是在什么时候提出来的，进而说明这不是一个新概念，这种讨论通常只有学术意义，对于认识新技术的本质并无太多实质性的帮助。讨论 SDN 的概念还是要从其真正的市场需求入手。

### 1．SDN 商用需求最早出现在数据中心内部

IDC 内部网络为了支持应用服务器上虚拟机的迁移，通常是一个二层网络，因为如果采用三层组网，那么虚拟机迁移时，虚拟机对应的应用服务的 IP 地址要跟着变化，带来业务部署和管理上的困难，而二层网络则没有这个问题。

但是，在 IDC 内部直接应用既有的二层网络技术则会带来以下两方面的问题：一个是在二层网络中，为了消除广播包的环路，通常采用生成树（STP）协议，在网络节点之间构建一棵逻辑树，节点之间的流量按照这个“树状”拓扑来传递，即使网络节点之间有多个物理链路，也只有一条链路真正传递数据，其他链路都是空闲的（只起备份作用）。但是，在 IDC 内部，多个服务器之间存在着频繁的数据交换需求，基于 STP 的树状网络拓扑不能高效支持这种“横向”流量，服务器之间的空闲链路也造成了网络资源的大量浪费，因此基于 STP 的二层网络对于 IDC 来说过

于简单，需要进行变革，尤其是随着云计算的发展，这种 IDC 内部二层组网需求越来越迫切。另一个问题是：通常 IDC 内部的应用服务器众多，有的达到上万台，甚至十几万台，二层交换机需要利用 ARP 等协议，学习接收到的数据包的源地址来建立 MAC 地址表，由于应用服务器多，所以 MAC 地址表项也多，通常会超过常规二层交换机 MAC 地址表的容量，造成大量 MAC 地址无法进入 MAC 地址表，二层交换机对于无法在 MAC 地址表中查到的 MAC 地址对应的数据帧进行二层域内的广播，造成二层网络内部的流量泛滥，影响 IDC 内部网络效率。

造成上述两个问题的根本原因是，传统的二层网络设计得过于简单，二层交换机只会学习 MAC 地址，不会基于 MAC 地址来规划数据转发路径。也就是说，传统二层网络中没有一个控制平面（或者说控制平面的功能非常弱，且与转发功能融合在一起），只有数据平面（负责数据帧的转发）。因此在二层网络中增加控制平面（或强化控制平面功能），负责较大的二层网络内部节点间的流量调度和管理成为一种迫切需求。目前主流的解决思路就是利用 IS-IS 路由协议的变种来构建控制平面路由功能；利用 Openflow 来定义控制平面与转发平面之间的接口。这就引出了控制平面与转发平面分离的概念。但这只是二层网络中的控制平面与转发平面的分离。

### 2. SDN 商用需求来自于路由器内部功能优化

在传统路由器中，负责路由规划、选路策略的控制平面与负责数据封装、高速转发的数据平面之间的接口是不开放的，是紧耦合在一起的。每个厂家都通过自有的协议或接口来连接控制平面和转发平面，这也是 CISCO、JUNIPER 等优势厂商维持技术壁垒、排挤新兴厂商的优势所在。

但是，有两方面的力量正在悄悄地对这种模式提出挑战：一个是大型互联网企业，它们有自建企业网络的需求，而且这些互联网企业认为目前自己企业网络的通信需求有特异性，而传统路由器的功能太复杂，有 80%以上的功能和特性在自己的网络中用不到，在购买这些路由器时却要为这些无用的功能买单，感觉比较“冤”，所以存在自主设计实现简洁高效路由器的需求，这也是 Facebook、Google、Yahoo 等公司发起成立 ONF（开放网络论坛），研制 SDN 标准的初衷之一。由于这些互联网企业具有在 IDC 内部大量采用自己定制的应用服务器的成功经验，所以它们对自主研发高效的路由器有着良好的期待。另一个力量是新兴的数据设备厂商，它们试图通过打破路由器内部控制平面与数据平面之间的紧耦合，形成一个开放的、标准的设备接口，这样可以把控制功能集中而且单独地剥离出去，这样数据转发设备可以做得更加通用和简单，成本可以更低，有助于打破 CISCO、JUNIPER 等厂商的垄断地位，从中获得新的发展机遇。

基于这种考虑，IETF 较早开展了路由器内部控制平面与转发平面分离的研究工作，成立了 FORCES 工作组，定义了路由器内部控制平面与转发平面之间的通信协议。这虽然同样引出了控制平面与转发平面分离的概念，但这是三层网络中的控制

平面与转发平面的分离。

### 3. SDN 商用需求来自未来网络研究与试验

目前，为了解决 IP 网络面临的网络地址空间不足、服务质量难以保证、安全可信机制缺乏、网络管控能力差等问题，未来网络研究人员一方面积极研究新型网络体系结构和关键技术，试图解决这些问题，目前虽然研究方向众多，但并未形成清晰的、共识的技术路线；另一方面，在技术路线不清楚、新方案层出不穷的情况下，有必要建立一个超大规模的未来网络新技术的试验验证环境（试验网络），在这个试验网络上灵活地为各种技术方案提供资源独立的试验环境，从而孵化出优选技术。美欧等分别建立了 GENI 和 FIRE 网络，目的就在于此。在试验网络建设过程中，设计人员希望能够在网络节点上灵活地控制和部署路由协议，实现高效的转发，因此形成了越来越强烈的、实验网节点上控制平面和转发平面分离的需求。通过控制平面的分离，可以实现网络控制功能的智能和集中，以及网络转发功能的协议无关和高效。

在实验网节点上控制平面和转发平面分离的情况下，每出现一种新的网络体系结构和解决方案，就可以在实现节点上以软件的形式来设计和配置，快速实现新的网络形态，高效支持网络技术创新与验证。

除了上述三种 SDN 需求及对应的三类专家以外，还有一些专家将 SDN 理解为统一智能网管，致力于实现一个可以统一、智能地管理多台网络设备的网管系统的目的，如在 LTE 的部署中，可以在 IP RAN 的设计中通过一个综合网管系统来配置和管理多台简化边缘路由器，从而提高网络策略部署效率。但是这种理解把管理平面从控制平面和数据平面中分离，不是控制平面和转发平面的分离，不应理解为是 SDN 技术。

## 6.1.2 “正本清源”SDN

前面分析了 SDN 的三种发展需求，综合来看，这些需求所追寻的都是网络“开放”的理念。

网络的开放是产业发展的必然趋势，不但能够带来相应设备和网络的高效性，而且可以进一步细分产业链，带来新的产业发展机遇。当年，机械零件之间的“开放”，实现了零件之间的标准互换，细化了机械加工的产业链，提高了成品机械的生产效率，极大地推动了工业革命的发展。在网络通信领域，通过 SDN 技术可以实现类似的期待。

在数据设备内，可以概括为两个平面，如图 6-1 所示。

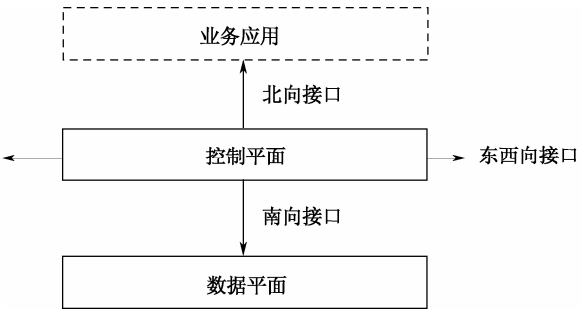



图 6-1　两个平面的分离

从网络开放性的角度来理解 SDN，可以把 SDN 分为三个类别，每个类别之间的开放性是递增的关系。

### 1. 开放控制层北向接口的 SDN（可以简称为 SDN-N）

这种思路研究数据网络开放控制面与业务应用之间的北向接口，向上提供资源抽象，实现软件可编程控制的网络架构。数据网络中控制层北向接口的开放有利于互联网应用服务感知数据网络状态、优化业务应用设计、改善用户业务体验，因此得到了互联网服务提供商的支持。北向接口开放性研究发端于 5 年前的 P2P 研究热潮，为了实现 P2P 流量优化与数据网络流量调度之间的协调，IETF 启动了 ALTO、DECADE 等多个工作组，随着 P2P 热度的消退，这些工作的研究进展缓慢，但是 SDN 的升温为这个研究方向注入了新的活力。研究北向接口的开放性，主要是要抽象不同业务应用的共性特征，及其对数据网络的承载需求，但是业务应用的多样性使得这项工作目前进展并不顺利。从纯学术的角度来看，北向接口的开放并没有涉及控制层与转发层的分离，因此一些专家认为这种技术思路不属于 SDN 研究范畴。

### 2. 开放控制层南向接口的 SDN（可以简称为 SDN-S）

这种思路就是通常理解的 SDN，即数据网络中控制平面与数据平面的分离。目前比较热的 ONF 的 Openflow 协议和 IETF 的 Forces 协议都是工作在这个层面的，都定义控制平面与数据平面分离后，两者之间的通信协议。Openflow 与 Forces 协议的不同点在于：Openflow 所面对的转发设备硬件假设只支持十元组，Openflow 可以针对十元组做各种转发规则的配置；而 Forces 假定所面对的转发设备硬件是协议无关的，Forces 可以以 XML 语言的格式来任意定义底层转发设备的处理逻辑。协议无关的转发设备目前也成为研究的热点，要做到协议无关，需要硬件具备众多功能，看似是十分困难的工作，但是一些芯片厂商和设备厂商已经研发出了协议无关的转发产品，这是一个值得关注的方向。

3. 开放控制层东西向接口的 SDN（可以简称为 SDN-SE）

在开放了南北向接口以后，SDN 发展中面临的一个问题就是控制平面的扩展性问题，也就是多个设备的控制平面之间如何协同工作，这涉及 SDN 中控制平面的东西向接口的定义问题。如果没有定义东西向接口，那么 SDN 充其量只是一个数据设备内部的优化技术，不同 SDN 设备之间还是要还原为 IP 路由协议进行互连，其对网络架构创新的影响力就十分有限。如果能够定义标准的控制平面的东西向接口，就可以实现 SDN 设备“组大网”，使得 SDN 技术走出 IDC 内部和数据设备内部，成为一种有革命性影响的网络架构。目前对 SDN 东西向接口的研究还刚刚起步，IETF 和 ITU 均未涉及这个研究领域。

从网络开放性的发展趋势来看，SDN 概念对网络设备和网络架构设计的影响还处于初级阶段，以后随着 SDN 中控制平面北向接口和东西向接口的标准化，以及 SDN 技术与网络虚拟化技术的融合，将使 SDN 技术释放出更大的活力和更为深远的影响力。

## 6.1.3 “任重道远”SDN

前面已经谈到，如果 SDN 技术和理念只是停留在目前 IDC 内部网络、数据设备内部，那么 SDN 技术的影响力是有限的，只是对二层网络内部的流量优化、数据设备结构和性能优化有较大的影响。但是如果 SDN 中的北向接口，尤其是东西向接口开放并且标准化以后，其对通信网网络结构、商业模式等均会产生深远的影响。目前业界热谈的 SDN 影响就是基于这种前提的。下面基于 SDN-SE 来谈谈 SDN 的影响。

（1）对于互联网企业而言。一方面，控制平面与转发平面的分离为网络控制权的迁移提供了机遇。目前 Google 等国际互联网巨头，绕过网络运营商，积极构建自主的网络基础设施，如购买海底光缆、部署光纤网络、发送“热气球”网络等。SDN 技术的出现，为互联网服务提供商（ISP）提供了构建廉价、高效网络的技术手段和机会。这不断对传统网络运营企业提出挑战，而且可能对互联网商业模式的发展产生重要影响。另一方面，SDN 技术优化了 IDC 内部网络，对于提高 IDC 效率、降低建设和运维成本具有重要意义。Google 等企业已经陆续发布了一些利用 SDN 技术后 IDC 效率大幅提升的事例和数据。IDC 的网络优化对于云计算的发展有着直接的促进作用。

（2）对设备制造企业而言。一方面，对于新兴厂商而言，SDN 意味着新的市场和商业机会，而且这是一片蓝海，这也是 NEC 等非主流数据设备厂商抢在 CISCO 等传统优势厂商之前研制发布 SDN 路由器和交换机的原因。另一方面，对于传统厂商而言，SDN 意味着垄断格局的打破，对于刺激技术创新和竞争、加快网络技术发

展具有重要的意义。

（3）对于网络运营商而言。一方面，SDN 为构建智能管道提供了技术途径，网络运营商可以利用 SDN 实现网络的优化和高效的管理，提高网络的智能性和管控能力，大幅降低网络建设与运维成本。另一方面，SDN 可以促进网络运营商真正开放底层网络，推动互联网业务应用的优化和创新。例如，在 OpenFlow 网络的支持下，IaaS 用户可以自行设定数据流在本网内的路径和安全策略，而不仅是几个虚拟设备的控制权。

（4）对于未来网络研究探索而言。一方面，在 SDN 等技术的推动和影响下，网络的虚拟化、控制转发分离成为未来网络新架构的基本特征，推动了未来网络体系结构和关键技术的创新。另一方面，SDN 技术为构建大规模未来网络试验床提供了基础技术，在试验网络中可以为新的网络技术方案提供相对独立的网络资源和网络控制功能，即在试验网上可自由定义数据的路由途径和转发交换规则，有利于网络技术创新。

另外，一些专家建议将 SDN 技术用于网络安全领域，利用 SDN 技术在基站或固网 POP 点中部署安全管控节点，实现安全管控节点的 CONTROLLER 之间的互连，构建网络安全边界（UNI/NNI 接口）。一是可以实现接纳控制、屏蔽用户对网络的攻击（IP 核心网络不可达）；二是便于安全规则的统一下发部署，可实现“群防群治”；三是与云计算相结合，自主发现异常流量，综合分析流量模式的特点，可以形成自发的“网络免疫系统”，实现“一点发现，全网免疫”；四是通过这些节点的互连，可以形成“应急通信系统”，实现网络的“应急通信”。

## 6.2　NDN（Named Data Networking）

面向内容的体系结构——基于名字的网络（NDN）[14][15]是美国国家科学基金委员会（NSF）重点资助的五个“未来互联网架构”（FIA）项目之一。当前互联网的主流业务是内容分发型业务，数据访问热度集中，而传统互联网架构采用端到端设计原则，缺乏数据热度感知和智能调度功能。用户业务模式与网络端到端流量调度之间的不匹配导致了网络上大量重复数据的传输，造成了相同内容的多次复制和相同流量的重复传输，进一步加剧了互联网网络流量负担。为了解决这个问题，NDN 的提出旨在设计新的网络体系结构，将网络通信从当前基于网络地址/位置的传输转变为基于网络内容的传输，解决当前互联网中存在的流量可扩展性、安全性、动态性等问题。

### 6.2.1　NDN 体系结构

NDN 依然采用 TCP/IP 网络的分层细腰结构，然而将细腰从 TCP/IP 体系结构中

的 IP 转变为了命名数据块（Named Content Chunks），如图 6-2 所示。另外，NDN 引入两个新的层次，即细腰之下的策略层（Strategy Iayer）和细腰之上的安全层（Security Iayer）。策略层进行转发及缓存决策，实现移动、多路径传输、网络缓存等，以更好地利用底层的多个并发连接（如以太网、3G 和 802.11）。安全层实现基于内容的安全，而不同于现有 TCP/IP 网络仅实现传输通道的安全保护，从而避免了现有互联网中存在的基于主机的多种网络攻击。

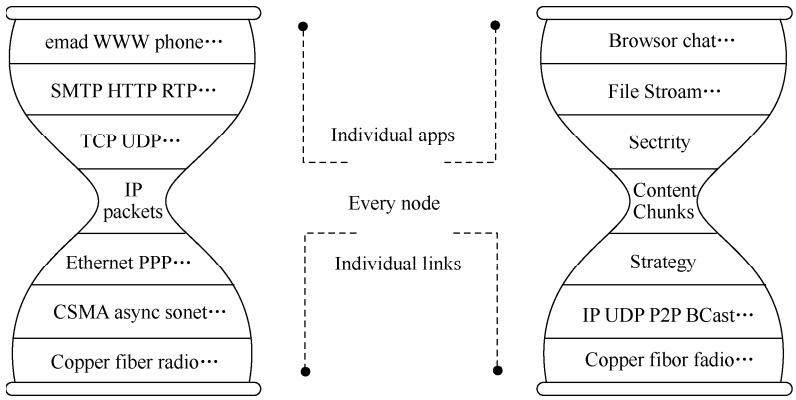



图 6-2　NDN 采用 TCP/IP 的分层细腰模型（细腰从 IP 转变为命名数据块）

## 6.2.2　NDN 节点模型

NDN 中，每个数据块都有唯一的名称，NDN 的通信是“Push-Pull”模型，即由内容的产生者和消费者共同驱动。网络中存在两种类型的分组：Interest 和 Data（见图 6-3）。数据的消费者需要获取某数据时，通过其所有可用的网络连接来广播 Interest 包，通过 Interest 包来请求该数据。任何网络节点接收到该 Interest 包且在本地有该 Interest 包所请求的数据时，通过 Data 包回复该请求。Interest 包和 Data 包通过数据的名字一一对应，Data 包仅作为相对应的 Interest 包的应答进行传输，并且会消耗掉该 Interest 包（即已经得到 Data 包应答的 Interest 包不再在网络中传输）。

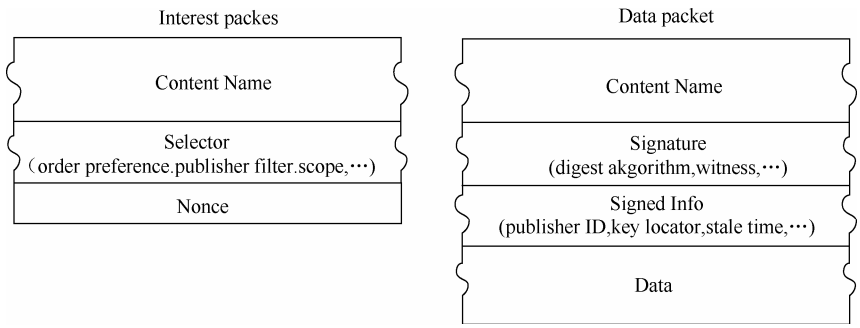



图 6-3　NDN 的两类分组

NDN 节点的基本操作类似于 IP 节点：分组到达节点的某个接口后，通过分组的名字进行最长匹配查找，根据查找结果执行相应的动作。图 6-4 所示为 NDN 分组转发引擎模型，包括三个主要的数据结构：FIB（Forwarding Information Base）、CS（Content Store，缓存）和 PIT（Pending Interest Table）。

FIB 表用来将 Internet 包转发给匹配数据的潜在数据源节点。除了 NDN 的 FIB 表的输出接口可以是不止一个外，其他方面与 IP 的 FIB 表的功能基本相同。这反映了在 NDN 中，Interest 包的转发路径不必是一棵生成树，Interest 包可以被转发给多个数据源节点，并行地向这些节点请求数据。

CS 用于缓存数据，从而在网络中增加缓存功能。NDN 的 CS 类似于 IP 路由器中的缓冲缓存，但采用了不同的替换策略。由于每个 IP 分组属于一个点到点的对话，分组在转发后将没有存在的意义，因此 IP 会“遗忘”掉已经转发的分组，在转发后立即回收它的缓冲区。NDN 中的分组是幂等的、自标识和自验证的，所以每个分组的内容都可能被其他用户重复使用（如许多用户在阅读相同的报纸或观看相同的 Youtube 视频）。为了最大化分享的概率，同时也为了最小化带宽及向下流传输的延迟，NDN 节点将尽量长时间地保留收到的数据（如使用 LRU 或 LFU 替换算法）。

PIT 表用于记录 Interest 分组向数据源节点转发的上行路径，从而使得被请求的数据（Data 分组）能够逆向地发送给请求者，各 NDN 节点的 PIT 表中记录已经被转发但是还没有得到相应的 Interests 分组的来源端口。在 NDN 中，只有 Interest 分组被路由，当 Interest 被转发给潜在的数据源时，就会留下一条“面包屑”。Data 分组将沿着“面包屑”指示的反向路径被传输给数据的请求者。每一条 PIT 都是一个面包屑。对于没有找到匹配 Data 分组的 Interest 信息，对应的 PIT 表项最终会超时（如果请求的发送者还想得到数据，则要重新发送 Interest 包）。

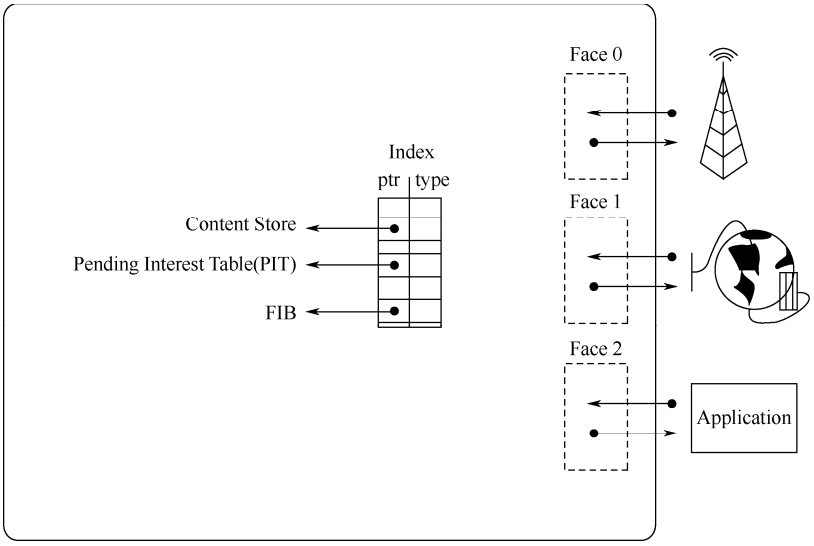



图 6-4　NDN 分组转发引擎模型

当一个 Interest 到达某个端口时，路由器将会根据它的 ContentName 进行一次最长匹配。查找的顺序依次是：CS 表、PIT 表和 FIB 表。如果在 CS 表中找到了匹配的项，则直接向接收 Interest 包分组的端口发送 Data 包，并且忽略该 Interest 包（因为该 Interest 包已经得到了响应）。

否则，如果在 PIT 表中存在一个完全匹配，则将接收该 Interest 包的端口加入到 PIT 表对应表项的转发列表中，并忽略该 Interest 包（当前，有一个或多个请求相同数据的 Interest 包已经被转发出去了，正在等待相应 Data 包的传输，所以当 Data 包被传输给该路由器时，该路由器可以将 Data 包转发给所有转发列表中的端口）。

如果 PIT 表不存在完全匹配，而存在一个 FIB 表的匹配，则 Interest 包需要根据 FIB 表项的发送列表传送给数据源，请求 Data 包。注意，如果 Interest 包到达的端口也在 FIB 表匹配的表项中，应该首先删除这个端口，然后转发给剩余的端口。

如果 FIB 表中也没有匹配，则丢弃这个 Interest 包（这个节点没有任何匹配的数据，也不知道如何找到数据）。

Data 包的处理相对简单，因为 Data 包不会被路由，而是简单地沿着 PIT 表项中记录的端口反向转发给原始的请求者。当 Data 包到达时，也要进行一次最长匹配。如果在 CS 表中存在匹配的内容，则说明 Data 包重复了，此时丢弃这个 Data 包。如果在 PIT 表中没有找到匹配项，则说明这个包没有被请求过，此时也丢弃这个包。如果在 PIT 表中存在匹配项，则说明这个 Data 包被请求过，则（有选择地）验证并添加到 CS 表中。PIT 表的匹配项的请求端口列表减去接收 Data 包的集合作为 Data 包的转发端口，将 Data 包转发出去。

这种基于 Interest 包的数据获取方式本身具有多点（multipoint）特性，这种特性为在高度动态的环境下保持通信提供了灵活性。任何同时接入多个网络的节点都可以作为一个内容路由器为多个网络服务。通过使用其缓存，移动节点可以成为两个无连接区域的传输介质，或者为时断链路提供延迟连接（类似 DTN）。这种 Interest/Data 包交换模式也在仅有本地连接时奏效。例如，在使用笔记本的两个同事，即使在没有接入 Internet 或企业网时，也能通过本地的 Ad hoc 网络共享文档。

### 6.2.3 NDN 技术的特点

NDN 重新设计了带着用户需求的架构，在这种架构中，漏斗模型的细腰被设定为命名的数据块。当前互联网的应用必须依赖复杂的中间层将指定 IP 的主机的抽象内容转化为需要的内容。NDN 大大简化了应用程序的开发，相对地，新的应用程序也会得到进一步的发展。

NDN 签名后的数据为未来网络的信任性建立了必要的基础。应用程序可以创建小颗粒的、自定义的验证、授权和信任模型。

NDN 中 Data 包的签名提供了数据完整性和数据来源的验证，所以当一个用户收到数据并验证了签名后，则用户确信收到的是来自正确的发布者的原数据的副本。因此，NDN 在不需要信息的发布者和客户直接交流的前提下，实现了安全的数据传输。

NDN 通过在每条路径上匹配 Data 包到 Interest 包，提供了一种每跳都会处理的强网络流量平衡方案。因此，NDN 网络可以在不依赖传输协议的基础上自我管理单播和多播的通信流量。另外，NDN 分离了路由规则和转发机制。

NDN 通过授权用户促进了网络的选择和竞争。在一些网络经济模型中已经被证实，监控信息交付的性能是确认 ISP 责任的关键。但是，在今天的全球路由系统中，IP 只选择单一的路径到达目标节点，由于“热土豆”路由的原因，这条路径通常是不对称的。这就导致当到达目的地址需要同时通过几个服务提供商时，很难测量和比较不同服务商的表现。作为对比，NDN 内置的多路线转发能力和反馈环使得用户可以探索多条路径，监视传递性能并最终作出选择。例如，在有多个网络连入接口的用户和小型服务商时，可以选择提供最好性能的服务商。这将会通过竞争鼓励网络架构中的创新和投资。

NDN 民主化了内容的分发，这是 NDN 显著地促进选择和竞争的另一个方式。传播内容和知识是互联网一个重要的社会影响。尽管今天的互联网无疑是成功的，但是今天互联网传播信息的能力相对于人们每天所创造内容的数量是远远不够的。NDN 自带的缓存能力使得信息创造者（无论是内容提供商还是个人用户）不需要任何特殊的架构（如 CDN）就能将信息高效地传播到全球的范围。特别是对于不发达的地区和不能充分发表意见群体的人来说，这将会造成深远的影响。这也将有一个积极的反馈效应，进一步鼓励人们去创造和产生原创信息。

## 6.3　NEBULA

NEBULA[17][18]也是 NSF 资助的五大 FIA 项目之一。NEBULA（希腊语中“云”的意思）是一个面向云计算数据中心互联的新型网络体系结构创新项目。Nebula 网络架构主要由三部分构成。

- NDP：NEBULA Data Plane；
- NVENT：NEBULA Virtual and Extensible Networking Techniques；
- NCore：NEBULA Core。

### 1．云数据平面（NDP）

NDP 是一个网络协议，这个协议中的每个包对于每个经过的管理域都包含以下四部分内容，如图 6-5 所示。

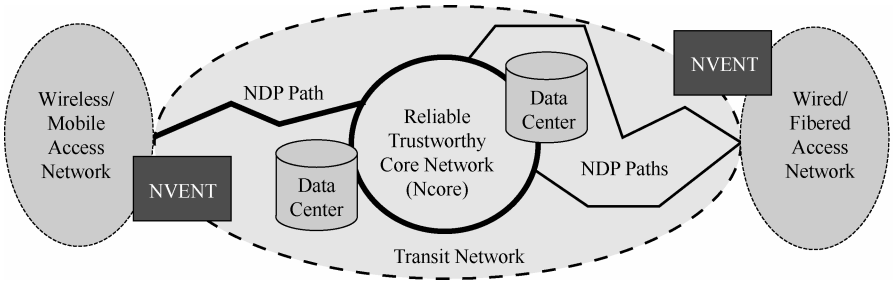



图 6-5　NEBULA 未来互联网架构模型

域的标识；

① PoC，该管理域已经授权了这条路径的证明；

② PoP，包遵循了其说明的路径的证明；

③ 多协议标签交换样式的标记。

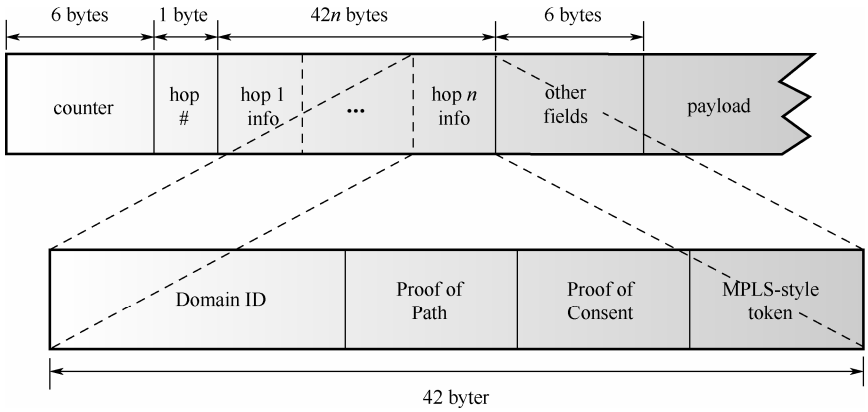



图 6-6　NDP 包格式

经过前期的调研发现[19][20]，这些元素不仅足以让网络中的元素表达自己的规则，而且可以执行相应的规则。当一个包到达一个自治域时，这个域有足够的信息来决定是否传递这个包：通过检查 PoC，确定这个包是否被授权；通过检查标记，确定这个包将会消耗哪些内部资源，经过了哪些中间组件；通过检查 PoP，确定这个包是否在授权的路径上传播。

前期的实验和原型已经证明，尽管这种架构占用了包空间、增加了数据平台的处理过程，但是具有很强的灵活性。

### 2. 云虚拟扩展组网技术（NVENT）

NVENT 的任务是当一个应用程序或提供商请求一个有某些需要的服务时，搜集可用的资源，并返回可用的路径及其他相关信息。

更具体地说，NVENT 的工作就是确定 NDP 包中各种参数的值。特别地，NVENT 负责决定包的传播路径，获取所有中间组件的许可，以及了解在这条路径上需要什么标识。通常来讲，发送者可以向 NVENT 服务器请求这些信息，并将它们放入包内。但是，更通常的做法是发送者发送和现在互联网相同的信息，代理服务器或网关向 NVENT 服务期请求信息，并将这些包转换为 NDP 包。这样，当 NDP 包进入网络时，各个自治域就有了足够的信息进行检查，具体如图 6-7 所示。

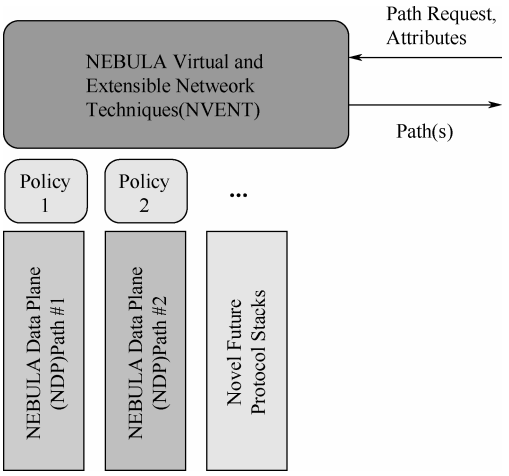



图 6-7　NVENT 用于路径选择的服务接口

### 3. 云核心网络（NCore）

NEBULA 的核心网络将会建立在下一代核心路由器之上，这些路由器将提供最快的传输速度，并且随时可用。而随时可用这个特性要求下一代的路由器的控制平台软件必须是一个可容错的分布式系统[21]。由于单核 CPU 不足以应对第一层 ISP 的数据转发，下一代的高性能路由器将会以分布式的形式存在。在未来，路由器将支持多插槽，每个插槽有多个网卡、转发服务器及控制服务器。路由器的各部分组件由高速光纤连接在一起，从外部来看，整个路由器就是一个小型的分布式系统，如图 6-8 所示。

除了高速稳定的路由器外，核心网络还需要数据中心和路由器之间的高速连接。Nebula 团队已经开始与思科和因特尔公司合作，探索数据中心和路由器之间的并行连接[22]，以提供高速可靠的连接。这将会解决数据中心中高速连接的网格存储和计算与核心网络中的广域网络之间的速度不匹配问题。同时，使用源地址和目的地址之间的多条路径[23]可以极大地改善传输带宽，也可以更好地应对网络中出现的线路或路由器的故障。在 NEBULA 中，将会创建一个和 NDP 机制相匹配的多路径路由协议，如图 6-9 所示。

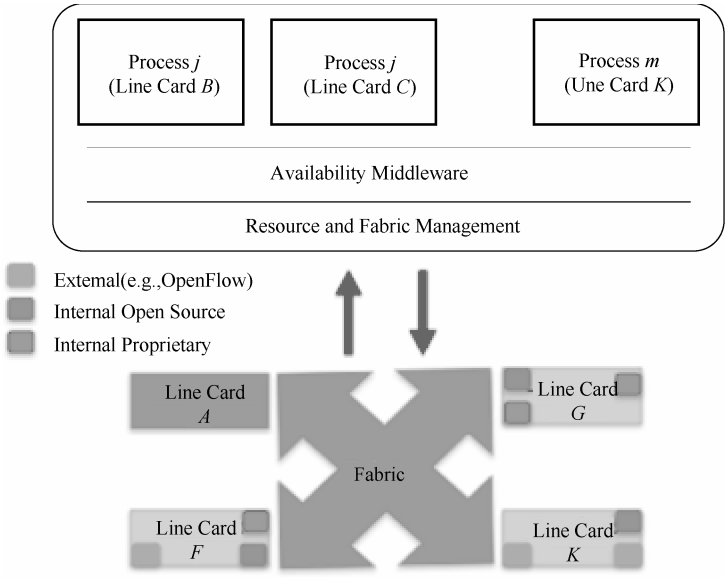



图 6-8　未来核心路由器的硬件和软件架构

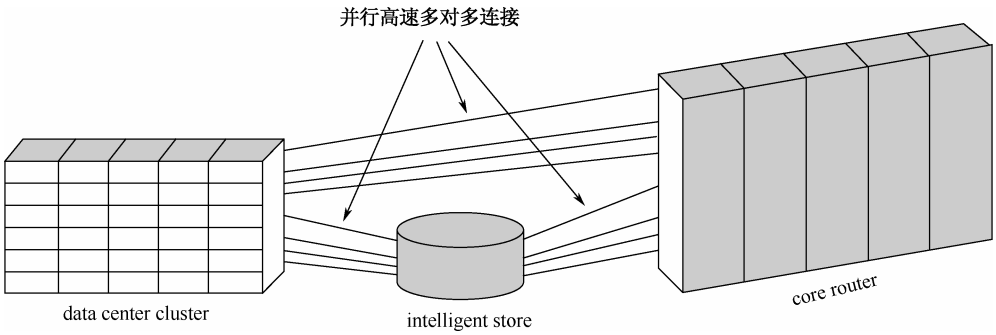



图 6-9　数据中心和核心网络之间的并行多对多的连接

## 6.4　XIA（eXpressive Internet Architecture）

XIA（eXpressive Internet Architecture）[24][25]也是美国 NSF 资助的五大 FIA 项目之一。XIA 致力于解决互联网应用模型日益增长的多样性和可信任通信问题，试图创造一个独立的网络，能够内在支持不同通信主体（包括现有互联网中主要的通信主体：主机、内容、服务，以及未来可能出现的各种新的通信主体）间的相互通信。XIA 针对每种通信主体定义一个特定的细腰（narrow waist），制定其用于通信的 API、网络通信机制及内生的安全机制。

## 6.4.1　XIA 技术思路

当前学术界已经提出了多种类型的通信方式，如内容为中心[14]、服务为中心[26][27]、多播[28]、支持移动性[16]等。XIA 的研究者认为应当提出一种框架，可以支持上述部分或全部功能，并且可以随时随地地选择支持或不支持这些功能。

为此，研究者提出了 XIA 网络架构。XIA 采用了当前互联网的“细腰”结构，但与当前互联网有多方面的不同：首先，当前互联网以主机为中心，XIA 则支持多种网络主体，包括主机、服务、内容，以及未来可能出现的新型主体；其次，XIA 支持网络架构的演进，提供了一种增量部署新功能的机制。XIA 主要基于下面三个核心概念。

### 1．多种网络主体

在以主机为中心的 TCP/IP 体系结构中，网络主体只有一种：主机。XIA 则支持多种多样的网络主体，包括主机、内容、服务，以及未来可能出现的新主体。XIA 支持新型主体的增量部署。应用程序能够使用不同类型的主体直接向网络表达它的需求，指示路由器对数据包执行特定的处理。除了更灵活的交互方式外，由于网络底层的功能直接被应用程序使用，也使得网络功能的优化更容易实现。

### 2．灵活的地址解析

XIA 支持网络架构的演进，支持新型主体增量部署的机制。XIA 引入了一种新的地址结构，通过灵活的地址解析使得旧系统能够兼容新主体。XIA 架构中的所有网络主体都有对应的 ID，应用程序请求网络提供的功能、内容和服务时，数据包的地址域中会填写主体的 ID。在 TCP/IP 架构中，数据包的源地址和目的地址只有一个，直接就是主机的 ID（IP 地址）。XIA 数据包地址域中填写的主体 ID 可以有多个，其中一个是首要主体，其余的是备用主体。

当路由器收到数据包时，按以下方式解析数据包的目的地址：首先查看首要主体，如果路由器自身支持这种主体类型，就直接按照主体类型相关的协议处理这个数据包；如果不支持首要主体的类型，就回退使用备用主体；备用主体可以有多个，解析的方式同上，如果不被支持就不断地回退。当在网络架构中引入一种新型主体时，将新型主体作为数据包地址域中的首要主体，同时将已被普遍支持的一种主体类型作为备用主体，这样，即使路由器无法识别该新型主体，也能根据备用主体正确地处理这个数据包。

### 3．内置安全性的 ID

XIA 要求网络中所有的主体 ID 都具有内置的安全性。主体 ID 的生成方式是与

主体类型相关的，其主体 ID 采用主机公钥的哈希值；内容获取的安全性主要表现为验证内容的正确性和完整性，其主体 ID 则采用内容本身的哈希值。通过内置安全性的 ID，网络实体（主机、路由器等）能够直接验证主体的安全性，不需要访问外部的数据库或配置信息。内置安全性的 ID 提供了一种基础性的安全机制，可以通过它构建更高层次的安全机制。

## 6.4.2 XIA 主体类型

在 XIA 架构中，通过使用多种主体类型，网络能够同时支持多种不同的通信方式，丰富网络架构的表达能力。XIA 在网络架构中增加了一种主体类型，其必须包括如下三方面的内容。

（1）该主体的通信语义

定义了主体类型的语义，即使用该主体类型进行通信的目的和意义，最常见的目的有获取特定的内容、与特定的主机通信。当一种通信方式无法用现有的主体类型有效地表达时，就可以考虑定义一种新的主体类型。

（2）该主体的 ID、ID 的生成方法和安全验证方法

主体 ID 的生成方法和安全性规则与主体的语义相关。例如，内容获取使用内容的哈希值，主机通信使用主机公钥的哈希值。根据主体的不同，XIA 至少有主机标识（HID）、服务 ID（SID）、内容标识（CID）等标识类型。

（3）路由器对主体数据包的处理

保证路由器等网络中间设备能正确处理数据包。在符合语义的前提下，路由器能够优化对数据包的处理，如缓存内容、支持任播。

# 参 考 文 献


[1] 钱华林，葛敬国，李俊. 层次交换网络体系结构. 北京：清华大学出版社.

[2] 张宏科，罗洪斌. 一体化可信网络与普适服务体系基础研究：目标、思路及进展. 技术与应用. 2008.12.

[3] 罗正海. 面向语义 Web 服务的本体合并研究. 硕士论文.

[4] 陈涛. IPv6 网络地址规划与实名可信通信关键技术和方法研究. 博士论文. 2010.

[5] ITU-T Y.2601，Fundamental characteristics and requirements of future packet based networks.

[6] ITU-T Y.2611，High-level architecture of future packet-based networks.

[7] ITU-T Y.2612，Generic requirements and framework of addressing, routing and forwarding in future, packet-based networks.

[8] ITU-T Y.2613，General technical architecture for public packet telecommunication data network.

[9] Towards the Future Internet，IOS Press BV.

[10] Named Data Networking（NDN）Project，Lixia Zhang, Deborah Estrin, and Jeffrey Burke，University of California.

[11] Internet Indirection Infrastructure，Ion Stoica Daniel Adkins Shelley Zhuang，University of California, Berkeley.

[12] The Future of the Internet，Pew Research Center.

[13] An Introduction to Virtualization on Planet Lab，Baris Metin.

[14] Implementing Network Virtualization for a Future Internet，Panagiotis Papadimitriou，Olaf Maennel，20th ITC Specialist Seminar 2009.

[15] Architectural Trends in Future Communication Systems，Donal O'Mahony.

[16] Future Internet Research and Experimentation，European Commission.

[17] http://ec.europa.eu/research/fp7/index_en.cfm.

[18] http://www.nets-find.net/.

[19] http://www.planet-lab.org/.

[20] 中国通信标准化协会（CCSA）研究课题（2012B81）. 未来互联网体系结构研究. 中国科学院计算技术研究所.

[21] 谢高岗，张玉军，李振宇，等. 未来互联网体系结构研究综述. 计算机学报. 2012，35（6）：1109−1119.

[22] http://www.huawei.com/broadband/iptime_backbone_solution/era/100g_transport_era.do, 2011.

[23] The CIDR Report, http://www.cidr-report.org.

[24] D. Meyer, L. Zhang, K. Fall. Report from the IAB workshop on routing and addressing. RFC 4984, 2007.

[25] G. Pallis and A. Vakali. Insight and Perspectives for Content Delivery Networks, Comm. of The ACM, 49（1）: 101-106, 2006.

[26] M.Meeker, S.Devitt, L.Wu. Internet trends. CM Summit, New York, 2010. http://www. morganstanley .com/institutional/techresearch.

[27] W.Gao, G.Cao. Fine-grained mobility characterization: steady and transient state behaviors. ACM Mobi Hoc2010.

[28] N.Azimi, H.Gupta, X.Hou, J.Gao. Data preservation under spatial failures in sensor networks, ACM Mobi Hoc2010.

[29] H.Xie, R.Yang, et al. P4P: provider portal for applications. ACM SIGCOMM2008.

[30] T.Karagiannis, K.Papagiannaki, M.Faloutsos. BLINC: multilevel traffic classification in the dark. ACM SIGCOMM2005.

[31] NSF Ne TS FIND Initiative, http://www.nets-find.net/.

[32] NSF Future Internet Architecture Project, http://www.nets-fia.net/.

[33] FIRE: Future Internet Research and Experimentation, http://cordis.europa.eu/fp7/ict/fire/.

[34] L.Zhang, D.Estrin, et al. Named data networking（NDN）project. PARC Technical Report NDN-0001, 2010. http://www.named-data.net/index.html.

[35] V. Jacobson, D. K. Smetters, et al. Networking named content. Communications of the ACM, 55（1）: 117-124, 2012.

[36] Seskar, Ivan, et al. "Mobilityfirst future internet architecture project." Proceedings of the 7th Asian Internet Engineering Conference. ACM, 2011.

[37] NEBULA: Future Internet Architecture, http://nebula-fia.org/.

[38] Anderson, Tom, et al. "The NEBULA Future Internet Architecture." The Future Internet. Springer Berlin Heidelberg, 2013. 16–26.

[39] Naous, Jad, et al. "Defining and enforcing transit policies in a future Internet." University of Texas at Austin Department of Computer Sciences Technical Report TR-10-07（2010）.

[40] Naous, Jad, et al. "The design and implementation of a policy framework for the future Internet." Submitted to the 2010 USENIX Symposium on Networked Systems Design and Implementation. 2009.

[41] Caesar, Matthew, et al. "Design and implementation of a routing control platform." Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation-Volume 2. USENIX Association, 2005.

[42] Traw, C. Brendan S., and Jonathan M. Smith. "Striping within the network subsystem." Network, IEEE 9.4（1995）: 22-32.

[43] Maxemchuk, Nicholas F. "Dispersity routing." Proceedings of ICC. 1975, 75.

[44] eXpressive Internet Architecture Project, http://www.cs.cmu.edu/～xia/.

[45] Dongsu Han, Ashok Anand, et al. XIA: Efficient Support for Evolvavle Internetworking. The 9th

USENIX Symposium on Networked Systems Design and Implementation（NSDI'12）, 2012.

[46] Nordstrom, Erik, et al. "Serval: An end-host stack for service-centric networking." Proc. 9th USENIX NSDI（2012）.

[47] Saif, Umar, and Justin Mazzola Paluska. "Service-oriented network sockets." Proceedings of the 1st international conference on Mobile systems, applications and services. ACM, 2003.

[48] Deering, Stephen E. Multicast routing in a datagram internetwork. No. STAN-CS-92-1415. STANFORD UNIV CA DEPT OF COMPUTER SCIENCE, 1991.

[49] Rouskas, George N., et al. "ChoiceNet: Network innovation through choice." ONDM. 2013.

[50] Anderson, Thomas, et al. "Overcoming the Internet impasse through virtualization." Computer 38.4（2005）: 34-41.

[51] Future Internet Assembly, http://www.future-internet.eu/home/future-internet-assembly.html.

[52] The FP7 4WARD Project, http://www.4ward-project.eu/.

[53] 吴建平，任罡，李星. 构建基于真实 IPv6 源地址验证体系结构的下一代互联网. 中国科学：E 辑 38.10（2008）: 1583−1593.

[54] CERNET Project, http://www.cernet.net/.

[55] 孟洛明. IP 网可测可控可管的研究现状和若干重要发展趋势. 通信学报. 29.12（2008）：96-101.

[56] XIE, Gaogang, et al. "Demo Abstract: Service-Oriented Future Internet Architecture（SOFIA）."

[57] Planet Lab Europe Project,http:// www.planet-lab.eu/.

[58] Magana, E., et al. "The European traffic observatory measurement infrastructure（ETOMIC）." IP Operations and Management, 2004. Proceedings IEEE Workshop on. IEEE, 2004.

[59] Tighe, Warren. "Network for integrating transportation operations systems（NITOS）." Vehicle Navigation and Information Systems Conference, 1995. Proceedings. In conjunction with the Pacific Rim Trans Tech Conference. 6th International VNIS.'A Ride into the Future'. IEEE, 1995.

[60] DIMES Projects,http://www.netdimes.org/new/.

[61] K-GENI Project,http://groups.geni.net/geni/wiki/K-GENI.

[62] Chun, Brent, et al. "Planet Lab: an overlay testbed for broad-coverage services." ACM SIGCOMM Computer Communication Review 33.3（2003）: 3-12.

[63] Global Environment for Network Innovations（GENI）Project, http://www.geni.net/.

[64] Fdida, Serge, Timur Friedman, and Thierry Parmentelat. "One Lab: An open federated facility for experimentally driven future internet research." New Network Architectures. Springer Berlin Heidelberg, 2010. 141−152.

[65] JGN2plus Project, http://www.jgn.nict.go.jp/.

[66] 邬江兴. 中国高性能宽带信息网（3TNet）综述. 通信世界. 2002，8.12: 37—39.

# 反侵权盗版声明